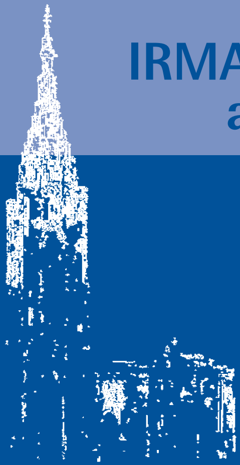

IRMA Lectures in Mathematics
and Theoretical Physics 28

Yann Bugeaud

Linear Forms in Logarithms and Applications

European Mathematical Society

IRMA Lectures in Mathematics and Theoretical Physics 28

Edited by Christian Kassel and Vladimir G. Turaev

Institut de Recherche Mathématique Avancée
CNRS et Université de Strasbourg
7 rue René Descartes
67084 Strasbourg Cedex
France

IRMA Lectures in Mathematics and Theoretical Physics
Edited by Christian Kassel and Vladimir G. Turaev

This series is devoted to the publication of research monographs, lecture notes, and other material arising from programs of the Institut de Recherche Mathématique Avancée (Strasbourg, France). The goal is to promote recent advances in mathematics and theoretical physics and to make them accessible to wide circles of mathematicians, physicists, and students of these disciplines.

For a complete listing see our homepage at www.ems-ph.org.

8 AdS/CFT Correspondence: Einstein Metrics and Their Conformal Boundaries, *Oliver Biquard* (Ed.)
9 Differential Equations and Quantum Groups, *D. Bertrand, B. Enriquez, C. Mitschi, C. Sabbah and R. Schäfke* (Eds.)
10 Physics and Number Theory, *Louise Nyssen* (Ed.)
11 Handbook of Teichmüller Theory, Volume I, *Athanase Papadopoulos* (Ed.)
12 Quantum Groups, *Benjamin Enriquez* (Ed.)
13 Handbook of Teichmüller Theory, Volume II, *Athanase Papadopoulos* (Ed.)
14 *Michel Weber*, Dynamical Systems and Processes
15 Renormalization and Galois Theory, *Alain Connes, Frédéric Fauvet and Jean-Pierre Ramis* (Eds.)
16 Handbook of Pseudo-Riemannian Geometry and Supersymmetry, *Vicente Cortés* (Ed.)
17 Handbook of Teichmüller Theory, Volume III, *Athanase Papadopoulos* (Ed.)
18 Strasbourg Master Class on Geometry, *Athanase Papadopoulos* (Ed.)
19 Handbook of Teichmüller Theory, Volume IV, *Athanase Papadopoulos* (Ed.)
20 Singularities in Geometry and Topology. Strasbourg 2009, *Vincent Blanlœil and Toru Ohmoto* (Eds.)
21 Faà di Bruno Hopf Algebras, Dyson–Schwinger Equations, and Lie–Butcher Series, *Kurusch Ebrahimi-Fard and Frédéric Fauvet* (Eds.)
22 Handbook of Hilbert Geometry, *Athanase Papadopoulos and Marc Troyanov* (Eds.)
23 Sophus Lie and Felix Klein: The Erlangen Program and Its Impact in Mathematics and Physics, *Lizhen Ji and Athanase Papadopoulos* (Eds.)
24 Free Loop Spaces in Geometry and Topology, *Janko Latschev and Alexandru Oancea* (Eds.)
25 *Takashi Shioya*, Metric Measure Geometry. Gromov's Theory of Convergence and Concentration of Metrics and Measures
26 Handbook of Teichmüller Theory, Volume V, *Athanase Papadopoulos* (Ed.)
27 Handbook of Teichmüller Theory, Volume VI, *Athanase Papadopoulos* (Ed.)

Yann Bugeaud

Linear Forms in Logarithms and Applications

European Mathematical Society

Author:

Yann Bugeaud
Université de Strasbourg, CNRS
Institut de Recherche Mathématique Avancée, UMR 7501
7, rue René Descartes
67084 Strasbourg CEDEX
France

E-mail: bugeaud@math.unistra.fr

2010 Mathematics Subject Classification: Primary: 11-02, 11J86, 11D; Secondary: 11B37, 11D25, 11D41, 11D59, 11D61, 11D75, 11D88, 11J25, 11J81, 11J82

Key words: Baker's theory, linear form in logarithms, Diophantine equation, Thue equation, *abc*-conjecture, primitive divisor, irrationality measure, *p*-adic analysis

ISBN 978-3-03719-183-5

The Swiss National Library lists this publication in The Swiss Book, the Swiss national bibliography, and the detailed bibliographic data are available on the Internet at http://www.helveticat.ch.

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in other ways, and storage in data banks. For any kind of use permission of the copyright owner must be obtained.

© 2018 European Mathematical Society

Contact address:

European Mathematical Society Publishing House
Seminar for Applied Mathematics
ETH-Zentrum SEW A21
CH-8092 Zürich
Switzerland

Email: info@ems-ph.org
Homepage: www.ems-ph.org

Typeset using the author's TEX files: Nicole Bloye, Cardiff, UK
Printing and binding: Beltz Bad Langensalza GmbH, Bad Langensalza, Germany
∞ Printed on acid free paper
9 8 7 6 5 4 3 2 1

Preface

Hay que saber buscar aunque uno no sepa qué es lo que busca.
Roberto Bolaño

— Les maths, m'sieur, ça fonctionne toujours à côté de ses grolles.
Jean Amila

In 1748 Leonhard Euler published *Introductio in analysin infinitorum* where, among several fundamental results, he established the relationship $\mathrm{e}^{\mathrm{i}\pi} = -1$ and gave explicitly the continued fraction expansions of e and e^2. He also made a conjecture concerning the nature of quotients of logarithms of rational numbers, which can be formulated as follows:

For any two positive rational numbers r, s with r different from 1, the number ${}^{\log s}/_{\log r}$ is either rational (in which case there are non-zero integers a, b such that $r^a = s^b$) or transcendental.

Recall that a complex number is called algebraic if it is a root of a non-zero polynomial with integer coefficients and a complex number which is not algebraic is called transcendental. Euler's conjecture implies, for example, that $2^{\sqrt{2}}$ is irrational (if it were rational, then $\log 2^{\sqrt{2}}$ divided by $\log 2$, which is equal to $\sqrt{2}$, would be rational or transcendental). It can be reformulated as follows:

If a is a positive rational number different from 1 and β an irrational real algebraic number, then a^β is irrational.

In 1900, David Hilbert proposed a list of twenty-three open problems and presented ten of them in Paris at the second International Congress of Mathematicians. His seventh problem expands the arithmetical nature of the numbers under consideration in Euler's conjecture and asks whether (observe that $\mathrm{e}^\pi = (-1)^{-\mathrm{i}}$)

the expression α^β for an algebraic base α different from 0 and 1 and an irrational algebraic exponent β, e.g. the number $2^{\sqrt{2}}$ or e^π, always represents a transcendental or at least an irrational number.

Here and below, unless otherwise specified, by algebraic number we mean complex algebraic number. Hilbert believed that the Riemann Hypothesis would be settled long before his seventh problem. This was not the case: the seventh problem was eventually solved in 1934, independently and simultaneously, by Aleksandr Gelfond and Theodor Schneider, by different methods. They established that, for any non-zero algebraic numbers $\alpha_1, \alpha_2, \beta_1, \beta_2$ with $\log \alpha_1$ and $\log \alpha_2$ linearly independent over the rationals (here and below, log denotes the principal determination of the logarithm function), we have

$$\Lambda_2 := \beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0.$$

Since the formulation is different, let us add some explanation. Under the hypotheses of Hilbert's seventh problem, the complex numbers $\log \alpha$ and $\log \alpha^\beta$ are linearly independent over the rationals and, assuming furthermore that α^β is algebraic, we derive from the Gelfond–Schneider theorem that β, equal to the quotient of the logarithm of α^β by the logarithm of α, cannot be algebraic, a contradiction.

Subsequently, Gelfond derived a lower bound for $|\Lambda_2|$ and, a few years later, he realized that an extension of his result to linear forms in an arbitrarily large number of logarithms of algebraic numbers would enable one to solve many challenging problems in Diophantine approximation and in the theory of Diophantine equations.

This program was realized by Alan Baker in a series of four papers published between 1966 and 1968 in the journal *Mathematika*. He made the long awaited breakthrough, by showing that, if $\alpha_1, \ldots, \alpha_n$ are non-zero algebraic numbers such that $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals, and if $\beta_1, \ldots, \beta_n$ are non-zero algebraic numbers, then

$$\Lambda_n := \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0.$$

In addition, he derived a lower bound for $|\Lambda_n|$, thereby giving the expected extension of the Gelfond–Schneider theorem. In his work, Baker generated a large class of transcendental numbers not previously identified and showed how the underlying theory can be used to answer a wide range of Diophantine problems, including the effective resolution of many classical Diophantine equations. He was awarded a Fields Medal in 1970 at the International Congress of Mathematicians in Nice.

It then became clear that further progress, refinements, and extensions of the theory would have important consequences. This area was at that time flourishing and developing very rapidly, both from a theoretical point of view (with improvements obtained by Baker and Feldman, among others, on the lower bounds for $|\Lambda_n|$) and regarding its applications. A spectacular achievement was the proof by Robert Tijdeman in 1976 that the Catalan equation $x^m - y^n = 1$, in the integer unknowns x, y, m, n all greater than 1, has only finitely many solutions (Preda Mihăilescu established in 2002 that $3^2 - 2^3 = 1$ is the only solution to this equation).

The aim of the present monograph is to serve as an introductory text to Baker's theory of linear forms in the logarithms of algebraic numbers, with a special emphasis on a large variety of its applications, mainly to Diophantine questions. We wish to help students and researchers to learn what is hidden inside the blackbox "Baker's theory of linear forms in logarithms" (in complex or in p-adic logarithms) and how this theory applies to many Diophantine problems.

Chapter 1 gives the reader a concise historical introduction to the theory. In Chapter 2, we gather several explicit lower bounds for $|\Lambda_n|$ and its p-adic analogue, which were established by Waldschmidt, Matveev, Laurent, Mignotte and Nesterenko, Yu, and Bugeaud and Laurent, and which will be used in the subsequent chapters. In all but one of these estimates, $\beta_1, \dots, \beta_n$ are integers, a special case sufficient for most of the applications. The lower bounds are then expressed in terms of the maximum B of their absolute values and take the form

$$\log|\Lambda_n| > -c(n, D)\,(\log 2A_1)\dots(\log 2A_n)\,(\log 2B),$$

where $c(n, D)$ is an explicit real number depending only on n and the degree D of the algebraic number field generated by $\alpha_1, \dots, \alpha_n$ and A_j is the maximum of the absolute values of the coefficients of the minimal defining polynomial of α_j over the rational integers, for $j = 1, \dots, n$. The crucial achievements of Baker are the logarithmic dependence on B and the fact that an admissible value for $c(n, D)$ can be explicitly computed.

We consider in Chapter 3 Diophantine problems for which the reduction to linear forms in complex logarithms is almost straightforward. These problems include explicit lower bounds for the distance between powers of 2 and powers of 3, effective irrationality measures for n-th roots of rational numbers, lower bounds for the greatest prime factor of $n(n+1)$, where n is a positive integer, perfect powers in linear recurrence sequences of integers, etc.

Chapter 4 is devoted to applications to classical families of Diophantine equations. In the works of Thue and Siegel, it was established that unit equations, Thue equations, and super- and hyperelliptic equations have only finitely many integer solutions, but the proofs were ineffective, in the sense that they did not yield upper bounds for the absolute values of the solutions and, consequently, were of very little help for the complete resolution of the equations. The theory of linear forms in logarithms induced dramatic changes in the field of Diophantine equations and we explain how it can be applied to establish, in an effective way, that unit equations, Thue equations, super- and hyperelliptic equations, the Catalan equation, etc., have only finitely many integer solutions. This chapter also contains a complete proof, following Bilu and Bugeaud [72], of an effective improvement of Liouville's inequality (which states that an algebraic number of degree d cannot be approximated by rational numbers at an order greater than d) derived ultimately from an estimate for linear forms in two complex logarithms proved in Chapter 11.

When the algebraic numbers $\alpha_1, \dots, \alpha_n$ occurring in the linear form Λ_n are all rational numbers very close to 1, the lower bounds for $|\Lambda_n|$ can be considerably improved. Several applications of this refinement are listed in Chapter 5. They include effective irrationality measures for n-th roots of rational numbers close to 1 and striking results on the Thue equation $ax^n - by^n = c$.

Chapter 6 presents various applications of the theory of linear forms in p-adic logarithms, in particular towards Waring's problem and, again, to perfect powers in linear recurrence sequences of integers. It also includes extensions of results established in Chapter 4: unit equations, Thue equations, super- and hyperelliptic equations have only finitely many solutions in the rational numbers, whose denominators are divisible by prime numbers from a given, finite set, and, moreover, the size of these solutions can be effectively bounded.

Primitive divisors of terms of binary recurrence sequences are discussed in Chapter 7. We partially prove a deep result of Bilu, Hanrot, and Voutier [77] on the primitive divisors of Lucas and Lehmer numbers and discuss some of its applications to Diophantine equations. Then, following Stewart [400], we confirm a conjecture of Erdős and show that, for every integer $n \geq 3$, the greatest prime factor of $2^n - 1$ exceeds some positive real number times $n\sqrt{\log n / \log\log n}$.

In Chapter 8, we follow Stewart and Yu [405] to establish partial results towards the abc-conjecture, which claims that, for every positive real number ε, there exists a positive real number $\kappa(\varepsilon)$, depending only on ε, such that, for all coprime, positive integers a, b, and c with $a + b = c$, we have

$$c < \kappa(\varepsilon) \Big(\prod_{p \mid abc} p \Big)^{1+\varepsilon},$$

the product being taken over the distinct prime factors of abc. Specifically, we show how to combine complex and p-adic estimates to prove the existence of an effectively computable positive real number κ such that, for all positive coprime integers a, b, and c with $a + b = c$, we have

$$\log c < \kappa \Big(\prod_{p \mid abc} p \Big)^{1/3} \Big(\log \Big(\prod_{p \mid abc} p \Big) \Big)^3.$$

There are only a few known applications of the theory of simultaneous linear forms in logarithms, developed by Loxton in 1986. Two of them are presented in Chapter 9. A first gives us an upper bound for the number of perfect powers in the interval $[N, N + \sqrt{N}]$, for every sufficiently large integer N. A second shows that, under a suitable assumption, a system of two Pellian equations has at most one solution.

Given a finite set of multiplicatively dependent algebraic numbers, we establish in Chapter 10 that these numbers satisfy a multiplicative dependence relation with small exponents. A key ingredient for the proof is a lower bound for the Weil height of a non-zero algebraic number which is not a root of unity.

Full proofs of estimates for linear forms in two complex logarithms, which, in particular, imply lower estimates for the difference between integral powers of real algebraic numbers, are given in Chapter 11. Analogous estimates for linear forms in two p-adic logarithms, that is, upper estimates for the p-adic valuation of the difference between integral powers of algebraic numbers are given in Chapter 12. An estimate for linear forms in an arbitrary number of complex logarithms is derived in Chapter 4 from the estimate for linear forms in two complex logarithms established in Chapter 11. While the former estimate is not as strong and general as the estimates stated in Chapter 2, it is sufficiently precise for many applications.

We collect open problems in Chapter 13. The thirteen chapters are complemented by six appendices, which, mostly without proofs, gather classical results on approximation by rational numbers, the theory of heights, algebraic number theory, and p-adic analysis.

We have tried, admittedly without too much success, to curb our taste for extensive bibliographies. No effort has been made towards exhaustivity, including in the list of bibliographic references, and the topics covered in this textbook reflect somehow the personal taste of the author.

Inevitably, there is some overlap between this monograph and the monograph [376] of Shorey and Tijdeman, which, although over thirty years old, remains an invaluable reference for anyone interested in Diophantine equations. In particular, the content of Chapter 4 (except Section 4.1) is treated in [376] in much greater generality. There is also some overlap with Sprindžuk's book [386] and the monograph of Evertse and Győry [182]. Regarding the theory of linear forms in logarithms, Chapters 2 and 11 can be seen as an introduction to the book of Waldschmidt [432]. As far as we are aware, the content of Chapters 5, 7, 8, 9, and 12 and several other parts of the present monograph have never appeared in books.

To keep this book reasonably short and accessible to graduate and post-graduate students, the results are not proved in their greatest generality and proofs of the best known lower bounds for linear forms in an arbitrary number of complex (*resp.*, p-adic) logarithms are not given.

Many colleagues sent me comments, remarks, and suggestions. I am grateful to all of them. Special thanks are due to Samuel Le Fourn, who very carefully read the manuscript and sent me many insightful suggestions.

This book was written while I was director of the 'Institut de Recherche Mathématique Avancée'.

Contents

Frequently used notation

log :	unless otherwise specified, $\log z$ denotes the principal determination of the logarithm of the non-zero complex number z, that is, writing $z = r\mathrm{e}^{\mathrm{i}\theta}$ with r positive and θ in $(-\pi, \pi]$, we have $\log z = \log r + \mathrm{i}\theta$.
e :	base of the natural logarithm.
deg :	degree (of a polynomial, of an algebraic number).
det :	determinant.
positive :	strictly positive.
$\lfloor x \rfloor$:	largest integer $\le x$.
$\lceil x \rceil$:	smallest integer $\ge x$.
$\{\cdot\}$:	fractional part.
$\lVert \cdot \rVert$:	distance to the nearest integer.
Card :	cardinality (of a finite set).
perfect power :	integer of the form a^b, with $a \ge 1$ and $b \ge 2$ integers.
$p_1 < p_2 < \cdots$:	the set of all prime numbers ranged in increasing order.
$q_1 < \cdots < q_s$:	a collection of s distinct prime numbers, not necessarily consecutive.
$P[n]$:	greatest prime factor of the integer n, with $P[0] = P[\pm 1] = 1$.
$\omega(n)$:	number of distinct prime factors of the positive integer n, with $\omega(1) = 0$.
φ :	Euler totient function (Definition D.3).
μ :	Möbius function (Definition D.3).
$\Phi_d(X, Y)$:	homogeneous d-th cyclotomic polynomial.
$h(\alpha)$:	logarithmic Weil height of the algebraic number α (Definition B.4).
$L(P)$:	length of the polynomial $P(X_1, \ldots, X_n)$ (Definition B.9).
$\lvert \cdot \rvert_p$:	p-adic absolute value, normalized such that $\lvert p \rvert_p = p^{-1}$.
v_p :	p-adic valuation, normalized such that $\mathrm{v}_p(p) = 1$.
S :	finite, non-empty set of prime numbers (or, sometimes, of places of an algebraic number field).

$[n]_S$: S-part of the non-zero integer n, defined by $[n]_S = \prod_{p \in S} |n|_p^{-1}$.

S-unit : rational number whose numerator and denominator are only composed of prime numbers in S.

integral S-unit : rational integer being an S-unit.

$a \ll b$: the quantity a is less than b times an absolute, positive, effectively computable real number.

$a \ll_{c_1,\ldots,c_n} b$: the quantity a is less than b times an effectively computable, positive, real number, which depends at most on $c_1, \ldots, c_n$.

$a \ll^{\text{ineff}} b$: the quantity a is less than b times an absolute, positive real number.

$\log_p, \exp_p$: p-adic logarithm and p-adic exponential functions.

$\mathcal{S}_N$: set of permutations of $\{1, \ldots, N\}$.

e_K, f_K : ramification index and residue degree of a p-adic field K.

$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{p}$: ideals of an algebraic number field.

$e_{\mathfrak{p}}, f_{\mathfrak{p}}$: ramification index and residue degree of an ideal $\mathfrak{p}$.

$\cdot^{\sigma}$: Galois conjugacy.

$K, O_K, O_K^*, M_K, M_K^{\infty}, D_K, h_K$: an algebraic number field, its ring of integers, group of units, set of places, set of infinite places, discriminant, and class number.

Chapter 1
Brief introduction to linear forms in logarithms

We start this textbook with a concise introduction to the theory of linear forms in logarithms. For much more comprehensive historical surveys and many bibliographic references, the reader is directed to the introductory text [441] and the monographs [28, 38, 141, 243, 419, 432]. Throughout, unless otherwise specified, $\log z$ denotes the principal determination of the logarithm of the non-zero complex number z, that is, writing $z = r\mathrm{e}^{\mathrm{i}\theta}$ with r positive and θ in $(-\pi, \pi]$, we have $\log z = \log r + \mathrm{i}\theta$. In particular, $\log(-1)$ is equal to $\mathrm{i}\pi$.

1.1. Linear forms in complex logarithms

A complex number is called algebraic if it is a root of a non-zero polynomial with integer coefficients. A complex number which is not algebraic is called transcendental. Rational numbers and their integer roots are obvious examples of algebraic numbers. The first examples of transcendental numbers were given, and even in a totally explicit form, by Liouville [264] in 1844, in a note where he proved that a real algebraic irrational number cannot be too close, in a suitable sense, to rational numbers; see Theorem A.5 for a precise formulation.

It is one thing to construct transcendental numbers; it is another, much more difficult one, to prove the transcendence of some explicitly given complex numbers. The first result in this direction is the proof of the transcendence of e, obtained by Hermite in 1873. Shortly thereafter, in 1882, Lindemann established that π is transcendental. The now famous Hermite–Lindemann theorem reads as follows.

THEOREM 1.1. *For any non-zero complex number β, at least one of the two numbers β and e^{β} is transcendental.*

Theorem 1.1 includes the transcendence of e (take $\beta = 1$) and that of π (take $\beta = \mathrm{i}\pi$). It also shows that $\log 2$ is transcendental and, more generally, that any determination of the logarithm of an algebraic number different from 0 and 1 is transcendental.

In 1885 Weierstrass extended Theorem 1.1 as follows.

THEOREM 1.2. *Let $n \ge 2$ be an integer. Let $\alpha_1, \dots, \alpha_n$ be distinct algebraic numbers. Then, $\mathrm{e}^{\alpha_1}, \dots, \mathrm{e}^{\alpha_n}$ are linearly independent over the field of algebraic numbers.*

Since monomials in $\mathrm{e}^{\alpha_1}, \dots, \mathrm{e}^{\alpha_n}$ are exponentials of integral combinations of $\alpha_1, \dots, \alpha_n$, it is easy to show that Theorem 1.2 is equivalent to the following statement: If $n \ge 2$

and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers that are linearly independent over the field of rational numbers, then $\mathrm{e}^{\alpha_1}, \ldots, \mathrm{e}^{\alpha_n}$ are algebraically independent over the field of algebraic numbers (this means that no non-zero polynomials with algebraic coefficients vanish at $(\mathrm{e}^{\alpha_1}, \ldots, \mathrm{e}^{\alpha_n})$).

In 1900, David Hilbert proposed a list of twenty-three open problems and presented ten of them in Paris at the second conference of the International Congress of Mathematicians. His seventh problem is the following (observe that $\mathrm{e}^{\pi} = (-1)^{-\mathrm{i}}$):

The expression α^{β} for an algebraic base α different from 0 and 1 and an irrational algebraic exponent β, e.g. the number $2^{\sqrt{2}}$ or e^{π}, always represents a transcendental or at least an irrational number.

This problem was solved in 1934 independently and simultaneously by Gelfond [197] and Schneider [359], by different methods.

THEOREM 1.3. *For any non-zero algebraic numbers $\alpha_1, \alpha_2, \beta_1, \beta_2$ with $\log \alpha_1$ and $\log \alpha_2$ linearly independent over the rationals, we have*

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0.$$

Theorem 1.3 was generalized to linear combinations of n logarithms of algebraic numbers by Baker [16, 17] in 1966 and 1967.

THEOREM 1.4. *Let $n \geq 2$ be an integer. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and* log *any fixed determination of the logarithm function. If $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals, then they are linearly independent over the field of algebraic numbers.*

Shortly thereafter, Baker [18] extended his previous result as follows.

THEOREM 1.5. *Let n be a positive integer. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and $\log \alpha_1, \ldots, \log \alpha_n$ any determinations of their logarithms. If $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals, then $1, \log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the field of algebraic numbers.*

It readily follows from Theorem 1.5 that the complex number $\mathrm{e}^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ is transcendental for all non-zero algebraic numbers $\alpha_1, \ldots, \alpha_n$, $\beta_0, \ldots, \beta_n$. Furthermore, Theorem 1.5 includes Theorem 1.1.

Theorems 1.3 to 1.5 show that any expression of the form

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n, \tag{1.1}$$

where $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ are non-zero algebraic numbers and β_0 is algebraic, vanishes only in trivial cases. A natural question is then to bound from below its absolute value (when non-zero).

For the sake of simplification, we assume in the discussion below that the algebraic numbers involved are all rational numbers. Let $n \geq 2$ be an integer. For $j = 1, \ldots, n$, let $\frac{x_j}{y_j}$ be a non-zero rational number, b_j a non-zero integer, and set

$$B := \max\{3, |b_1|, \ldots, |b_n|\} \quad \text{and} \quad A_j := \max\{3, |x_j|, |y_j|\}. \tag{1.2}$$

We consider the rational number

$$\Lambda := \Bigl(\frac{x_1}{y_1}\Bigr)^{b_1} \cdots \Bigl(\frac{x_n}{y_n}\Bigr)^{b_n} - 1. \tag{1.3}$$

Since we wish to bound $|\Lambda|$ from below, we may assume that $|\Lambda| \le \frac{1}{2}$. Then, the *linear form in logarithms of rational numbers* Ω, defined by

$$\Omega := \log(1 + \Lambda) = b_1 \log \frac{x_1}{y_1} + \cdots + b_n \log \frac{x_n}{y_n},$$

satisfies

$$\frac{|\Lambda|}{2} \le |\Omega| \le 2|\Lambda|.$$

A trivial estimate of the denominator of (1.3) gives that $\Lambda = 0$ or

$$\log|\Lambda| \ge -\sum_{j=1}^{n} |b_j| \log\max\{|x_j|, |y_j|\} \ge -B \sum_{j=1}^{n} \log A_j. \tag{1.4}$$

The dependence on the A_j's in (1.4) is very satisfactory, unlike the dependence on B. For applications to Diophantine problems, we require a better estimate in terms of B than the one given in (1.4), even if it comes with a weaker one in terms of the A_j's. For example, replacing B by $o(B)$ is sufficient in many cases (see, for example, Theorems 3.10, 3.13, and 4.9), but not in all cases (see, for example, Theorems 3.3, 3.4, and 5.1). The next lemma shows that B cannot be replaced by $o(\log B)$.

Lemma 1.6. *Let $n, a_1, \ldots, a_n$ be integers, all of which are greater than or equal to 2. Set $A = \max\{a_1, \ldots, a_n\}$. Then, for every integer B greater than $2n \log A$, there exist rational integers $b_1, \ldots, b_n$ with*

$$0 < \max\{|b_1|, \ldots, |b_n|\} \le B$$

and

$$|a_1^{b_1} \cdots a_n^{b_n} - 1| \le \frac{2n \log A}{B^{n-1}}.$$

Lemma 1.6 is a direct consequence of the Dirichlet *Schubfachprinzip* applied to the points $b_1 \log a_1 + \cdots + b_n \log a_n$ with $0 \le b_1, \ldots, b_n \le B$, which all lie in the interval $[0, nB \log A]$.

The first effective improvement of (1.4) was obtained by Gelfond [198] in 1935 in the case $n = 2$. He proved that, for multiplicatively independent positive rational numbers $\frac{x_1}{y_1}, \frac{x_2}{y_2}$, for an arbitrary positive real number ε, and for all integers b_1, b_2, not both 0, we have

$$\Bigl|\Bigl(\frac{x_1}{y_1}\Bigr)^{b_1} \Bigl(\frac{x_2}{y_2}\Bigr)^{b_2} - 1\Bigr| \gg_{\frac{x_1}{y_1}, \frac{x_2}{y_2}, \varepsilon} \exp\bigl(-(\log B)^{5+\varepsilon}\bigr),$$

where $B = \max\{3, |b_1|, |b_2|\}$. Throughout this book, the notation $a \gg_{c_1,\ldots,c_n} b$ (*resp.*, $a \gg^{\text{ineff}}_{c_1,\ldots,c_n} b$) means that the quantity a is greater than b times an effectively computable positive real number (*resp.*, a positive real number), which depends at most on $c_1, \dots, c_n$. Subsequently, Gelfond improved his own result and totally explicit estimates were provided by Schinzel [354] in 1967.

Gelfond [200] also gave an estimate valid for a linear form in an arbitrary number of logarithms.

Theorem 1.7. *Let $n \geq 2$ be an integer and $a_1, \dots, a_n$ positive rational numbers which are multiplicatively independent. Let δ be a positive real number. Let $b_1, \dots, b_n$ be rational integers, not all zero, and set $B = \max\{3, |b_1|, \dots, |b_n|\}$. Then, we have*

$$|a_1^{b_1} \cdots a_n^{b_n} - 1| \gg^{\text{ineff}}_{n, a_1, \dots, a_n, \delta} \exp(-\delta B).$$

The proof of Theorem 1.7, which rests on a theorem of Siegel, does not enable us to compute effectively the implicit numerical constant. In his book Gelfond [200] pointed out the importance of getting an effective version of Theorem 1.7.

For $n \geq 3$, the first non-trivial effective lower bound for the quantity Λ defined in (1.3) was given by Baker [16] in 1966. With B as in (1.2), he obtained that either $\Lambda = 0$ or, for every positive real number ε, we have

$$\left|\left(\frac{x_1}{y_1}\right)^{b_1} \cdots \left(\frac{x_n}{y_n}\right)^{b_n} - 1\right| \gg_{n, \frac{x_1}{y_1}, \dots, \frac{x_n}{y_n}, \varepsilon} \exp\bigl(-(\log B)^{n+1+\varepsilon}\bigr).$$

His result is much more general and applies to expressions of the form (1.1).

Shortly thereafter, Feldman [185, 186] established the following refinement of Baker's lower bound.

Theorem 1.8. *Let $n \geq 2$ be an integer and $a_1, \dots, a_n$ positive rational numbers which are multiplicatively independent. Let $b_1, \dots, b_n$ be rational integers, not all zero, and set $B = \max\{3, |b_1|, \dots, |b_n|\}$. Then, there exists a positive, effectively computable real number C, depending only on $n, a_1, \dots, a_n$, such that*

$$|a_1^{b_1} \cdots a_n^{b_n} - 1| \geq \exp(-C \log B) = B^{-C}. \tag{1.5}$$

Lemma 1.6 shows that the dependence on B in the estimate (1.5) is essentially best possible, but, for applications, it is much desirable to determine precisely how C depends on the rational numbers $a_1, \dots, a_n$.

A first explicit result in this direction was given by Baker [19] in 1968. Throughout this chapter, the height of an algebraic number is the naïve height, that is, the maximum of the absolute values of the coefficients of its minimal defining polynomial over the integers. We reproduce below a consequence of the main theorem of [19].

Theorem 1.9. *Assume that $n \geq 2$ and that $\alpha_1, \dots, \alpha_n$ are non-zero algebraic numbers, whose degrees do not exceed D and whose heights do not exceed A, where $D \geq 4$ and $A \geq 4$. Let δ be a real number with $0 < \delta \leq 1$. Let $b_1, \dots, b_n$ be rational integers, not all zero, and set $B = \max\{3, |b_1|, \dots, |b_n|\}$. If*

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| < \frac{\mathrm{e}^{-\delta n B}}{2},$$

then

$$B < (4^{(n+1)^2} \delta^{-1} D^{2(n+1)} \log A)^{(2n+3)^2}.$$

In many applications, especially to classical families of Diophantine equations, we are led to bound from below expressions of the form $|\alpha_1^{b_1} \cdots \alpha_n^{b_n} \alpha_{n+1} - 1|$, where α_{n+1} has a large height; see Chapter 4. In this respect, Theorem 1.9 is not plainly satisfactory, since $\alpha_1, \ldots, \alpha_n$ play the same rôle, irrespective of their height and their exponent. Its following refinement, established by Baker [26], appears to be very useful.

Theorem 1.10. *Assume that $n \geq 1$ and let $\alpha_1, \ldots, \alpha_{n+1}$ be non-zero algebraic numbers of degree at most D. Let the heights of $\alpha_1, \ldots, \alpha_n$ and α_{n+1} be at most A and A_{n+1} respectively, where $A \geq 2$ and $A_{n+1} \geq 2$. Let δ be a positive real number. Let $b_1, \ldots, b_n$ be integers, not all zero, and set $B = \max\{3, |b_1|, \ldots, |b_n|\}$. If*

$$0 < |\alpha_1^{b_1} \cdots \alpha_n^{b_n} \alpha_{n+1} - 1| < \mathrm{e}^{-\delta B},$$

then

$$B \ll_{n,D,A,\delta} \log A_{n+1}.$$

In the present textbook, we give a complete proof of Theorem 1.10. We derive it from a lower bound for linear forms in two logarithms; see Section 4.1.

In 1975, Baker [27] established a subsequent refinement of Theorem 1.8.

Theorem 1.11. *Assume that $n \geq 2$ and that $\alpha_1, \ldots, \alpha_n$ are non-zero algebraic numbers, whose degrees do not exceed D. Assume that, for $j = 1, \ldots, n$, the height of α_j does not exceed A_j, where $A_j \geq 2$. Let $b_1, \ldots, b_n$ be rational integers, not all zero, and set $B = \max\{3, |b_1|, \ldots, |b_n|\}$. If $\alpha_1^{b_1} \cdots \alpha_n^{b_n}$ is not equal to 1, then*

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| > B^{-C\,\Pi \log \Pi}, \tag{1.6}$$

where

$$\Pi = \log A_1 \cdots \log A_n$$

and C is an effectively computable real number depending only on n and D.

As was pointed out by Baker below the statement of his theorem, *it would be of much interest to eliminate* $\log \Pi$ in (1.6). Also, Theorem 1.11 does not include Theorems 1.9 and 1.10, nor the main result of Baker's paper [25].

The deletion of the $\log \Pi$ factor (which is mainly interesting from a theoretical point of view, but also has several applications, see, for example, Theorem 3.6) has been achieved independently by Wüstholz [440] and by Philippon and Waldschmidt [329]. Thus, at the end of the '80s, it was established that, with Λ, $A_1, \ldots, A_n$, and B as in (1.2) and (1.3), there exists an effectively computable real number $c(n)$, depending only on the number n of rational numbers involved in (1.3), such that the lower estimate

$$\log\left|\left(\frac{x_1}{y_1}\right)^{b_1} \cdots \left(\frac{x_n}{y_n}\right)^{b_n} - 1\right| \geq -c(n) \log A_1 \cdots \log A_n \log B \tag{1.7}$$

holds, when Λ is non-zero. Since then, several authors have managed to considerably reduce the value of the real number $c(n)$. However, it remains an open problem to replace the product $\log A_1 \cdots \log A_n$ by the sum $\log A_1 + \cdots + \log A_n$; see Chapter 13.

1.2. Linear forms in p-adic logarithms

Let p be a prime number. In parallel with the development of the theory of linear forms in complex logarithms, progress has been regularly made towards its p-adic analogue.

For a non-zero rational number x, let $\mathrm{v}_p(x)$ denote the exponent of p in the decomposition of x as a product of prime powers. With $\Lambda, A_1, \dots, A_n$, and B as in (1.2) and (1.3), a trivial estimate shows that

$$\mathrm{v}_p\Big(\Big(\frac{x_1}{y_1}\Big)^{b_1}\cdots\Big(\frac{x_n}{y_n}\Big)^{b_n}-1\Big) \le \frac{\log(2A_1^{b_1}\cdots A_n^{b_n})}{\log p} \le 1+\frac{B}{\log p}\sum_{j=1}^{n}\log A_j. \qquad (1.8)$$

The theory of p-adic linear forms in logarithms gives a much better result in terms of the dependence on B, namely, that there exists an effectively computable real number $c'(n)$, depending only on the number n of rational numbers involved, such that the upper estimate

$$\mathrm{v}_p\Big(\Big(\frac{x_1}{y_1}\Big)^{b_1}\cdots\Big(\frac{x_n}{y_n}\Big)^{b_n}-1\Big) \le c'(n)\; p\; \log A_1\cdots\log A_n \log B \qquad (1.9)$$

holds, when Λ is non-zero. In terms of B, this is much better than (1.8) and analogous to (1.7). One of the major open problems in the theory is to remove (or at least to improve) the dependence on p in (1.9), which remains very unsatisfactory and is ultimately a consequence of the fact that the radius of convergence of the p-adic exponential function is finite.

A good reference for an historical introduction is [448]. Mahler [278] established in 1932 the p-adic analogue of the Hermite–Lindemann theorem and three years later [280] the p-adic analogue of the Gelfond–Schneider theorem. Gelfond [199] proved a quantitative estimate for linear forms in two p-adic logarithms, which was later refined by Schinzel [354].

Estimates for linear forms in an arbitrary number of p-adic logarithms were obtained by Brumer [99], Sprindžuk [384, 385], Coates [149], Kaufman [238], Baker and Coates [34], van der Poorten [335], Dong [168, 169], and Yu [443, 445–447], among others.

1.3. Linear forms in elliptic logarithms

A few years after the birth of the theory of linear forms in logarithms, it was realized that the techniques used in the proofs can be applied to any commutative algebraic group. Initial steps towards the derivation of elliptic analogues were made by Baker [23], who considerably extended earlier results of Schneider [360]. Elliptic curves with complex multiplication were studied by Masser [284] in 1975 and, a year later, Coates and Lang [151] established the first lower bounds in the case of Abelian varieties with complex multiplication. Subsequently, Philippon and Waldschmidt [330] and Hirata-Kohno [229, 230] obtained rather general statements.

In the case of elliptic logarithms, the first totally explicit estimates were given by David [162]. These have applications to the complete determination of the integral points on an elliptic curve, as is very well explained by Stroeker and Tzanakis [408], Gebel, Pethő, and Zimmer [196], and Tzanakis [420, 421].

Let n be a positive integer and $E_1, \dots, E_n$ elliptic curves over an algebraic number field K. For $j = 1, \dots, n$, consider a Weierstrass model of E_j and $\wp_j$ the associated Weierstrass function. Let u_j be a complex number such that $\wp_j(u_j)$ is in $K \cup \{\infty\}$. Such a complex number u_j is an elliptic logarithm of an algebraic point of E_j. Also, let $\beta_0, \beta_1, \dots, \beta_n$ be elements of K. Let $B \geq 3$ denote an upper bound for the heights of $\beta_0, \beta_1, \dots, \beta_n$.

Set

$$\Lambda_e := \beta_0 + \beta_1 u_1 + \cdots + \beta_n u_n.$$

David and Hirata-Kohno [163] established that there exists an effectively computable positive real number c, which depends only on $K, n, u_1, \dots, u_n$ and the curves $E_1, \dots, E_n$, such that we have $|\Lambda_e| \geq B^{-c}$ if Λ_e is non-zero.

For the state-of-the-art and generalisations to Abelian varieties, the reader is directed to [163] and to Gaudron's papers [192–194].

Lower bounds for linear forms in p-adic elliptic logarithms were given by Rémond and Urfels [345] and Hirata-Kohno and Takada [232]; see also Fuchs and Pham [189].

Chapter 2
Lower bounds for linear forms in complex and p-adic logarithms

We list below several estimates for linear forms in complex and p-adic logarithms, which will be used throughout the book. We give only few bibliographic references and direct the reader to the monograph of Waldschmidt [432] for further information, in particular to its Section 10.4. Most of the results quoted are corollaries of more precise estimates, so the reader wishing to apply the theory of linear forms in logarithms should better consult the original papers to find the sharpest bounds available to date.

In this chapter we write completely explicit estimates. This will, however, not be the case for most of the results presented in the next chapters, where we will often make no effort to give explicit values for the numerical constants. Throughout, h denotes the (logarithmic) Weil height; see Definition B.4.

2.1. Lower bounds for linear forms in complex logarithms

We start with a general theorem of Waldschmidt [430,432] on inhomogeneous linear forms in logarithms of algebraic numbers with algebraic coefficients.

Theorem 2.1. *Let $n \geq 1$ be an integer. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers. Let* $\log \alpha_1, \ldots, \log \alpha_n$ *be determinations of their logarithm and assume that* $\log \alpha_1, \ldots, \log \alpha_n$ *are linearly independent over the rationals. Let $\beta_0, \ldots, \beta_n$ be algebraic numbers, not all zero. Let D be the degree over $\mathbb{Q}$ of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_0, \ldots, \beta_n)$. Let E, E^*, and $A_1, \ldots, A_n$ be real numbers with*

$$E^* \geq E^{1/D} \geq \mathrm{e}^{1/D}, \quad E^* \geq \mathrm{e}, \quad E^* \geq \frac{D}{\log E},$$

and

$$\log A_j \geq \max\left\{h(\alpha_j), \frac{E}{D}|\log \alpha_j|, \frac{\log E}{D}\right\}, \quad 1 \leq j \leq n.$$

Let B^* be a real number with

$$B^* \geq E^*, \quad B^* \geq \max_{1 \leq j \leq n} \frac{D \log A_j}{\log E}, \quad \log B^* \geq \max_{0 \leq j \leq n} h(\beta_j).$$

Then, we have

$$\log |\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n| \\ \geq -2^{n+25}\, n^{3n+9}\, D^{n+2} \log A_1 \ldots \log A_n \log B^* \log E^* (\log E)^{-n-1}.$$

Assume that we are in the homogeneous rational case, that is, assume that $\beta_0 = 0$ and $\beta_1, \ldots, \beta_n$ are rational integers $b_1, \ldots, b_n$ with $b_n \neq 0$. Let B' be a real number satisfying

$$B' \geq E^*, \quad B' \geq \max_{1 \leq j \leq n-1} \Big\{ \frac{|b_n|}{\log A_j} + \frac{|b_j|}{\log A_n} \Big\}.$$

Then, we have

$$\log |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| \\ \geq -2^{n+26}\, n^{3n+9}\, D^{n+2} \log A_1 \ldots \log A_n \log B' \log E^* (\log E)^{-n-1}.$$

In particular, choosing $E = \mathrm{e}$ and $E^* = 3D$, we get

$$\log |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| \\ \geq -2^{n+26}\, n^{3n+9}\, D^{n+2} \log(3D) \log A_1 \ldots \log A_n \log B'.$$

Proof. This follows from Theorem 9.1 of [432], taking into account Remark 3 on page 303 and Proposition 9.18 of [432]. □

By Proposition 9.21 of [432], the assumption in Theorem 2.1 that $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals can be relaxed to the assumptions $\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0$ and

$$D^3 (\log B_0)(\log A_j)(\log E^*) \geq (\log D)(\log E)^2, \quad 1 \leq j \leq n,$$

where $B_0 = B^*$ in the general case and $B_0 = B'$ in the homogeneous rational case.

Theorem 2.1 plainly includes Theorem 1.5. It also contains Theorem 1.11 and the lower bound (1.7). Taking $n \geq 2$ and $b_n = 1$ in the homogeneous rational case of Theorem 2.1 and setting $B := \max\{3, |b_1|, \ldots, |b_{n-1}|\}$, we get

$$-\log |b_1 \log \alpha_1 + \cdots + b_{n-1} \log \alpha_{n-1} + \log \alpha_n| \ll_{n,D} \log A_1 \ldots \log A_n \log\Big(\frac{B}{\log A_n}\Big).$$

This has many important applications, in particular to Diophantine equations; see Theorems 4.1, 4.3, and 4.5. Assuming that there exists a real number δ such that $0 < \delta \leq \frac{1}{2}$ and $|b_1 \log \alpha_1 + \cdots + b_{n-1} \log \alpha_{n-1} + \log \alpha_n| < \mathrm{e}^{-\delta B}$, we deduce that

$$B \ll_{n,D} \delta^{-1} \log A_1 \ldots \log A_{n-1} \log\big(\delta^{-1} \log(D^{n-1} A_1 \ldots A_{n-1})\big) \log A_n.$$

This (and the discussion below explaining how the linear form (2.1) and the quantity (2.2) are related) shows that Theorem 2.1 also contains Theorem 1.10.

In the homogeneous rational case, a result similar to Theorem 2.1 was proved independently by Baker and Wüstholz [37, 38]. Since their estimate (which has a better dependence on n than in Theorem 2.1, namely the factor n^{3n} is replaced by n^{2n}) does not include the useful parameters E and B', and is superseded by Theorem 2.2 below, we do not quote it.

The parameter E originates in papers by Shorey [367, 368] and is of interest when $\alpha_1, \dots, \alpha_n$ are real and very close to 1, in which case it can be chosen to be very large. By assumption, $\log E$ cannot exceed $D \min_{1 \le j \le n} \log A_j$. However, in some cases, it can be taken close to this quantity. To see this in the homogeneous rational case, assume that, for $j = 1, \dots, n$, we have $\alpha_j = 1 + \frac{1}{x_j}$, for an integer $x_j \ge 3$. Then, setting

$$E = E^* = \min_{1 \le j \le n} x_j \quad \text{and} \quad A_j = x_j + 1, \quad 1 \le j \le n,$$

we see that, since $B' \ge E$, Theorem 2.1 implies the lower bound

$$\log |b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| \gg_n - \frac{\log A_1 \dots \log A_n}{(\min_{1 \le j \le n} \log A_j)^{n-1}} \cdot \log \max\{3, |b_1|, \dots, |b_n|\}.$$

In the most favourable cases, for example when there exists a real number M such that $\max_{1 \le j \le n} x_j \le (\min_{1 \le j \le n} x_j)^M$, we get

$$\log |b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| \gg_n -M^{n-2} \Big(\max_{1 \le j \le n} \log A_j \Big) \log \max\{3, |b_1|, \dots, |b_n|\},$$

thus replacing the product of the $\log A_j$, as it occurs in the statement of Theorem 2.1, with their maximum. Further explanations are given below Theorem 2.5, in Chapter 5, and in Section 10.4.3 of [432].

In the course of this textbook, we mention in passing a few applications of the first assertion of Theorem 2.1 (at the beginning of Section 3.3 and in Section 3.10), but we only apply estimates for homogeneous linear forms in logarithms with integer coefficients. Therefore, we focus our attention on the second assertion of Theorem 2.1 and its subsequent improvements and refinements.

Let $n \ge 2$ be an integer. Let $\alpha_1, \dots, \alpha_n$ be non-zero algebraic numbers. Let $b_1, \dots, b_n$ be integers. Let $\log \alpha_1, \dots, \log \alpha_n$ be any determination of the logarithms of $\alpha_1, \dots, \alpha_n$. The theory of linear forms in logarithms provides us with lower bounds for the absolute value of the linear form

$$b_1 \log \alpha_1 + \dots + b_n \log \alpha_n, \tag{2.1}$$

when it is non-zero. This yields lower bounds for the quantity

$$|\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1|, \tag{2.2}$$

which occurs frequently in Diophantine questions. We choose below to mainly consider quantities of the form (2.2) and not (2.1). When $\alpha_1, \dots, \alpha_n$ are all real numbers, both forms are essentially equivalent since $\log(1 + x) = x + O(x^2)$ in the neighborhood of the origin. This is however not the case when complex non-real numbers are among $\alpha_1, \dots, \alpha_n$. Indeed, denoting by log the principal determination of the logarithm, to say that (2.2) is small does not imply that $b_1 \log \alpha_1 + \dots + b_n \log \alpha_n$ is close to 0, but merely that $b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$ is close to an integer multiple of $2i\pi$. Precisely, we derive the existence of an integer b_0 with $|b_0| \leq |b_1| + \cdots + |b_n|$ and such that the linear form

$$b_0 \log(-1) + b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$$

is close to 0.

The next statement is a corollary of the, at present time, best known general estimate, due to Matveev [290, 291]. The crucial improvement on the earlier results [37, 430] concerns the dependence on the number n of logarithms: it is exponential in n, and not of the form n^{cn} as in the earlier estimates.

Theorem 2.2. *Let $n \geq 1$ be an integer. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers. Let D be the degree over $\mathbb{Q}$ of a number field containing $\alpha_1, \ldots, \alpha_n$. Let $A_1, \ldots, A_n$ be real numbers with*

$$\log A_j \geq \max\left\{h(\alpha_j), \frac{|\log \alpha_j|}{D}, \frac{0.16}{D}\right\}, \quad 1 \leq j \leq n.$$

Let $b_1, \ldots, b_n$ be integers and set

$$B = \max\{|b_1|, \ldots, |b_n|\}$$

and

$$B'' = \max\left\{1, \max\left\{|b_j| \frac{\log A_j}{\log A_n} : 1 \leq j \leq n\right\}\right\}.$$

Then, we have

$$\log |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| > -3 \times 30^{n+4} (n+1)^{5.5} D^{n+2} \log(eD) \log A_1 \ldots \log A_n \log(enB) \tag{2.3}$$

and, if $n \geq 2$ and $\alpha_1, \ldots, \alpha_n$ are all real numbers, we get the better lower bound

$$\log |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| > -2 \times 30^{n+3} n^{4.5} D^{n+2} \log(eD) \log A_1 \ldots \log A_n \log(eB). \tag{2.4}$$

The same statements hold with B replaced by $\max\{B'', nB\pi/(D \log A_n)\}$ in (2.3) and with B replaced by B'' in (2.4).

Proof that Theorem 2.2 follows from Matveev's results. Inequality (2.4) with B replaced or not by B'' is an immediate consequence of Corollary 2.3 of Matveev [291]. Denote by log the principal determination of the logarithm. If $|\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| < \frac{1}{2}$, then there exists an integer b_0, with $|b_0| \leq n\, B$, such that

$$\Omega := |b_0 \log(-1) + b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n|$$

satisfies $|\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| \geq \frac{\Omega}{2}$. Noticing that $|\log(-1)| = \pi$ and $h(-1) = 0$, we set $\log A_0 = \frac{\pi}{D}$ and deduce (2.3) from Corollary 2.3 of Matveev [291].

Since

$$|b_0| \frac{\log A_0}{\log A_n} \leq \frac{nB\pi}{D \log A_n},$$

we see that B can be replaced by $\max\{B'', nB\pi/(D \log A_n)\}$ in (2.3). □

We stress that the definition of B' in Theorem 2.1 is slightly different from that of B'' in Theorem 2.2. The lower bound (2.4) with B'' in place of B is crucial for the proof of Theorem 3.8.

Many Diophantine problems can be reduced to lower bounds for linear forms in two or three logarithms. While, in the case of three logarithms, we do not have very satisfactory estimates (but see [298]), Laurent, Mignotte, and Nesterenko [254] obtained in 1995 rather sharp lower bounds for linear forms in two logarithms. The quality of their result is an illustration of the method of interpolation determinants, which was introduced in this context by Laurent [252]. The current best known estimates have been established by Laurent in 2008 in [253]. We display below an estimate obtained in Corollary 1 of [253] and three consequences of the main result of [254].

Theorem 2.3. *Let α_1 and α_2 be multiplicatively independent algebraic numbers. Set $D' = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]$. Let A_1 and A_2 be real numbers such that*

$$\log A_j \geq \max\Big\{h(\alpha_j), \frac{1}{D'}, \frac{|\log \alpha_j|}{D'}\Big\}, \quad j = 1, 2.$$

Let b_1 and b_2 be integers, not both zero, and set

$$\log B' = \max\Big\{\log\Big(\frac{|b_1|}{D' \log A_2} + \frac{|b_2|}{D' \log A_1}\Big) + 0.21, \frac{20}{D'}, 1\Big\}.$$

Then, we have the lower bound

$$\log |b_1 \log \alpha_1 + b_2 \log \alpha_2| \geq -25.2\, D'^4 (\log A_1)(\log A_2)(\log B')^2. \tag{2.5}$$

For $n = 2$, the numerical constant in (2.4) exceeds 10^9. It has been substantially reduced in Theorem 2.3. This is crucial for applications to the complete resolution of Diophantine equations. Very roughly speaking, when a Diophantine problem can be reduced to linear forms in only two logarithms, then it can (often, this is not always true! See Problem 13.12) be completely solved.

A weaker version (weaker only in terms of the numerical constants) of Theorem 2.3 is proved in this book; see Theorem 11.1. Note also that, unlike in Theorem 2.3, the algebraic numbers α_1 and α_2 are not assumed to be multiplicatively independent in Theorem 11.1. This allows us to deduce directly from Theorem 2.3 a slightly weaker version of Theorem 2.6, see Theorem 11.3.

Observe that the dependence on B' in Theorem 2.3 is not best possible and worse than in Theorems 2.1 and 2.2, since $\log B'$ occurs squared. Gouillon [202] established a lower bound for $|b_1 \log \alpha_1 + b_2 \log \alpha_2|$, where the dependence on B' occurs through a factor $(\log B')$ only. His numerical constants being not so small, it is better for most of the applications to use the bounds established in [253, 254]. However, to have the best possible dependence in B' is essential for the proofs of Theorems 3.3 and 5.1.

As in Theorem 2.1, an extra parameter E was introduced in [254]. We reproduce below Corollaire 3 of [254].

Theorem 2.4. *Let α_1 and α_2 be multiplicatively independent positive real algebraic numbers. Let D be the degree of the number field $\mathbb{Q}(\alpha_1, \alpha_2)$. Let A_1 and A_2 be real* *numbers such that*

$$\log A_j \geq \max\Big\{h(\alpha_j), \frac{1}{D}, \frac{|\log \alpha_j|}{D}\Big\}, \quad j = 1, 2.$$

Let b_1 and b_2 be integers, not both zero. Let E be a real number with

$$E \leq 1 + \min\Big\{\frac{D\log A_1}{|\log \alpha_1|}, \frac{D\log A_2}{|\log \alpha_2|}\Big\} \tag{2.6}$$

and set

$$\log B' = \max\Big\{\log\Big(\frac{|b_1|}{D\log A_2} + \frac{|b_2|}{D\log A_1}\Big) + \log\log E + 0.47, \frac{10\log E}{D}, \frac{1}{2}\Big\}.$$

Assume furthermore that $2 \leq E \leq \min\{A_1^{3D/2}, A_2^{3D/2}\}$. Then,

$$\log|b_1\log\alpha_1 + b_2\log\alpha_2| \geq -35.1D^4(\log A_1)(\log A_2)(\log B')^2(\log E)^{-3}.$$

In [254], the authors defined the parameter E to be equal to the right hand side of (2.6). However, it easily follows from the proof that Theorem 2.4 as stated is correct.

A weaker version (weaker only in terms of the numerical constants) of Theorem 2.4 is proved in this book; see Theorem 11.2.

The following consequence of Theorem 2.4 emphasizes the rôle of the parameter E in a particular case which occurs frequently in applications.

Theorem 2.5. *Let x_1, x_2, y_1, y_2 be positive integers with $x_1 \geq 2$, $x_1 \neq y_1$, and $y_2 < x_2 \leq \frac{6}{5}y_2$. Let b be a positive integer and assume that $(\frac{x_1}{y_1})^b \neq \frac{x_2}{y_2}$. Define the parameter η by*

$$\frac{x_2}{y_2} = 1 + x_2^{-\eta}.$$

Then, we have $\eta\log x_2 > 1$ and

$$\log\Big|\Big(\frac{y_1}{x_1}\Big)^b\frac{x_2}{y_2} - 1\Big| \geq -\frac{35.2}{\eta}(\log x_1)\Big(\max\Big\{1 + \frac{\log b}{\eta\log x_2}, 10\Big\}\Big)^2. \tag{2.7}$$

Since $\frac{x_2}{y_2} > 1$, we always have $\eta < 1$. The estimate is stronger when η is very close to 1, that is, when $\frac{x_2}{y_2}$ is very close to 1. Under the assumption of Theorem 2.5, we get instead of (2.5) a lower bound of the form

$$\gg -\frac{(\log A_1)(\log A_2)}{-\log(\frac{x_2}{y_2} - 1)} \cdot (\log B')^2,$$

with $A_1 = \max\{x_1, 3\}$ and $A_2 = \max\{x_2, 3\}$. This crucial improvement upon the “classical” estimate (2.5) turns out to have many spectacular applications, some of which being given in Chapter 5; see Theorems 5.2, 5.4, and 5.6.

Proof of Theorem 2.5 assuming Theorem 2.4. If $y_1 > x_1$, then the left hand side of (2.7) exceeds $\log(\frac{y_1}{x_1} - 1)$, thus it exceeds $-\log x_1$ and (2.7) holds.

If $y_1 < x_1$ and $x_1 \leq 5$, then $(\frac{y_1}{x_1})^b \leq \frac{4}{5}$ and (2.7) holds since $\frac{x_2}{y_2} \leq \frac{6}{5}$.

If $x_1 > y_1$ and $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ are multiplicatively dependent, then there exist coprime positive integers c, d and positive integers u, v such that $\frac{x_1}{y_1} = (\frac{c}{d})^u$ and $\frac{x_2}{y_2} = (\frac{c}{d})^v$. We then get

$$\Big|\Big(\frac{y_1}{x_1}\Big)^b \frac{x_2}{y_2} - 1\Big| = \Big|\Big(\frac{d}{c}\Big)^{ub-v} - 1\Big| \geq \frac{1}{\max\{c, d\}} \geq \frac{1}{x_1},$$

and the theorem holds.

Thus, we assume that $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ are multiplicatively independent, $x_1 > y_1$, and $x_1 \geq 6$. Observe that (2.7) holds if $x_1 < x_2^\eta/2$. To see this, it suffices to observe that, since $y_1 < x_1$, we then get

$$0 < \Big(\frac{y_1}{x_1}\Big)^b \frac{x_2}{y_2} \leq \Big(1 - \frac{1}{x_1}\Big)\Big(1 + \frac{1}{x_2^\eta}\Big) < 1 - \frac{1}{2x_1},$$

which implies that

$$\Big|\Big(\frac{y_1}{x_1}\Big)^b \frac{x_2}{y_2} - 1\Big| \geq \frac{1}{2x_1}.$$

Thus, in the sequel, we assume that $x_2^\eta \leq 2x_1$. We apply Theorem 2.4 with $\alpha_1 = \frac{x_1}{y_1}$ and $\alpha_2 = \frac{x_2}{y_2}$. Then, $D = 1$, $A_1 = x_1$ and $A_2 = x_2$ (note that the assumption $y_2 < x_2 \leq \frac{6}{5} y_2$ implies that $x_2 \geq 6$). Furthermore, we set

$$E = x_2^\eta.$$

Observe that $E \geq 5$, since $5x_2 \leq 6y_2$. This proves the first assertion of the theorem. Furthermore, we have $E \leq \min\{x_1^{3/2}, x_2^{3/2}\}$, since $x_1 \geq 6$ and $\eta < 1$.

We deduce from $\log(1 + x_2^{-\eta}) \leq x_2^{-\eta}$ that

$$1 + \frac{\log x_2}{\log \frac{x_2}{y_2}} = 1 + \frac{\log x_2}{\log(1 + x_2^{-\eta})} \geq 1 + x_2^\eta \log x_2 \geq E.$$

Furthermore, we may assume that

$$\Big|\Big(\frac{y_1}{x_1}\Big)^b \frac{x_2}{y_2} - 1\Big| \leq x_1^{-10},$$

since otherwise the theorem clearly holds. Using this inequality and $5 \leq x_2^\eta \leq 2x_1$, we deduce that

$$b \log \frac{x_1}{y_1} \leq \log \frac{x_2}{y_2} + 2x_1^{-10} \leq x_2^{-\eta} + 2^{11} x_2^{-10\eta} \leq 2x_2^{-\eta},$$

thus

$$1 + \frac{\log x_1}{\log \frac{x_1}{y_1}} \geq 1 + \frac{b}{2} x_2^\eta \log x_1 \geq E,$$

since $x_1 \geq 6$. Consequently, we have checked that

$$E \leq 1 + \min\Big\{\frac{\log x_1}{\log \frac{x_1}{y_1}}, \frac{\log x_2}{\log \frac{x_2}{y_2}}\Big\}.$$

The assumptions of Theorem 2.4 are then satisfied and we derive that

$$\begin{aligned}\log\Bigl|\log\Bigl(\frac{x_2}{y_2}\Bigr) - b\log\Bigl(\frac{x_1}{y_1}\Bigr)\Bigr| &\ge -35.1\,(\log x_1)\,\Bigl(\frac{\log x_2}{\log E}\Bigr)\,\Bigl(\frac{\log B'}{\log E}\Bigr)^2\\ &\ge -\frac{35.1}{\eta}\,(\log x_1)\,\Bigl(\frac{\log B'}{\log E}\Bigr)^2,\end{aligned}$$

where

$$\begin{aligned}\frac{\log B'}{\log E} &= \max\left\{\frac{\log\bigl(\frac{b}{\log x_2}+\frac{1}{\log x_1}\bigr)}{\log E} + \frac{\log\log E + 0.47}{\log E}, 10\right\}\\ &\le \max\Bigl\{1 + \frac{\log b}{\eta\log x_2}, 10\Bigr\}.\end{aligned}$$

We conclude by using that every real number z with $|z| \le \frac{1}{2}$ satisfies $|\log(1+z)| \le 2|z|$. This completes the proof of the theorem. □

For some applications, we need a lower bound for quantities of the shape $|\alpha^b - 1|$, where α is a complex algebraic number of modulus 1. Such an estimate does not follow from Theorem 2.3, since in its statement α_1 and α_2 are assumed to be multiplicatively independent. We display a consequence of Théorème 3 of [254].

Theorem 2.6. *Let α be a complex algebraic number of modulus 1 which is not a root of unity. Let b be a positive integer. Set*

$$D' = \frac{[\mathbb{Q}(\alpha):\mathbb{Q}]}{2}, \qquad \log A = \max\Bigl\{\frac{20}{D'}, 11\frac{|\log\alpha|}{D'} + h(\alpha)\Bigr\},$$

and

$$\log B' = \max\Bigl\{\frac{17}{D'}, \frac{1}{10\sqrt{D'}}, \log\frac{b}{25} + 2.35 + \frac{5.1}{D'}\Bigr\}.$$

Then, we have

$$\log|\alpha^b - 1| \ge -9(D')^3\,(\log A)(\log B')^2.$$

Proof that Theorem 2.6 follows from Théorème 3 of [254]. Recall that log denotes the principal determination of the logarithm. If $|\alpha^b - 1| < \frac{1}{3}$, then there exists an integer b_0 with $|b_0| \le b$ such that

$$|\alpha^b - 1| \ge \frac{|b_0\log(-1) + b\log\alpha|}{2}.$$

We then use the inequalities

$$\frac{1}{2D'\log A} + \frac{1}{68.9} \le \frac{1}{40} + \frac{1}{68.9} \le \frac{1}{25}$$

to get from Théorème 3 of [254] that

$$\log|b_0\log(-1) + b\log\alpha| \ge -8.87(D')^3\,(\log A)(\log B')^2.$$

This yields the desired estimate. □

2.2. Multiplicative dependence relations between algebraic numbers

The results displayed in the previous section provide us with lower bounds for the quantity

$$|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n|,$$

when it is non-zero. However, in some situations, we derive linear forms in logarithms that are equal to zero. It is then often useful to find rational integers $b_1', \ldots, b_n'$, not all zero, with small absolute values and such that

$$b_1' \log \alpha_1 + \cdots + b_n' \log \alpha_n = 0.$$

A result of this type was given by Loxton and van der Poorten [271]. We quote below a version of Waldschmidt [432].

Theorem 2.7. *Let $m \geq 2$ be an integer and $\alpha_1, \ldots, \alpha_m$ multiplicatively dependent non-zero algebraic numbers. Let $\log \alpha_1, \ldots, \log \alpha_m$ be any determination of their logarithms. Let D be the degree of the number field generated by $\alpha_1, \ldots, \alpha_m$ over $\mathbb{Q}$. For $j = 1, \ldots, m$, let A_j be a real number satisfying*

$$\log A_j \geq \max\Big\{h(\alpha_j), \frac{|\log \alpha_j|}{D}, 1\Big\}.$$

Then there exist rational integers $n_1, \ldots, n_m$, not all zero, such that

$$n_1 \log \alpha_1 + \cdots + n_m \log \alpha_m = 0$$

and

$$|n_j| \leq \big(11(m-1)D^3\big)^{m-1} \frac{(\log A_1) \cdots (\log A_m)}{\log A_j}, \quad \text{for } j = 1, \ldots, m.$$

A full proof of Theorem 2.7, together with additional references, is given in Chapter 10. Theorem 2.7 is used in the proof of Theorem 3.16.

2.3. Lower bounds for linear forms in p-adic logarithms

Let p be a prime number and K an algebraic number field. Let O_K denote the ring of integers of K. Let $\mathfrak{p}$ be a prime ideal in K, lying above the prime number p, and denote by $e_{\mathfrak{p}}$ its ramification index, that is, the exponent of $\mathfrak{p}$ in the decomposition of the ideal pO_K in a product of prime ideals; see Section B.1. For a non-zero algebraic number α in K, let $\mathrm{v}_{\mathfrak{p}}(\alpha)$ denote the exponent of $\mathfrak{p}$ in the decomposition of the fractional ideal αO_K in a product of prime ideals and set

$$\mathrm{v}_p(\alpha) = \frac{\mathrm{v}_{\mathfrak{p}}(\alpha)}{e_{\mathfrak{p}}}.$$

This defines a valuation v_p on K which extends the p-adic valuation v_p on $\mathbb{Q}$ normalized in such a way that $\mathrm{v}_p(p) = 1$.

Let $\alpha_1, \dots, \alpha_n$ be elements of K and $b_1, \dots, b_n$ non-zero rational integers. We look for an upper bound for the quantity

$$\mathrm{v}_p(\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1),$$

where $b_1, \dots, b_n$ denote rational integers, not all zero, when $\alpha_1^{b_1} \dots \alpha_n^{b_n}$ is not equal to 1.

We begin with an easy estimate.

Theorem 2.8. *Let p be a prime number, $b \geq 2$ an integer, and α an algebraic number of degree D. If α^b is not equal to* 1*, then*

$$\mathrm{v}_p(\alpha^b - 1) < \frac{\log b}{\log p} + 2D\frac{p^D - 1}{\log p} h(\alpha) + 2D\frac{\log 2}{\log p}.$$

The proof of Theorem 2.8 is given in Section B.3. Theorem 2.8 is trivial unless $\mathrm{v}_p(\alpha) = 0$, in which case the factor $(p^D - 1)$ corresponds to the upper bound for the smallest positive integer s such that $\mathrm{v}_p(\alpha^s - 1)$ is positive. The dependence on p in Theorem 2.8 was slightly improved by Yamada [442] by means of a subtle variation of the proof of the main estimate of [129] for linear forms in two p-adic logarithms. Yamada's result, reproduced as Theorem 12.3 and established in Chapter 12, has a striking application to an old conjecture of Erdős; see Theorem 7.11.

The next result is a slight simplification of the estimate given on page 190 of Yu's paper [449].

Theorem 2.9. *Let p be a prime number and $\alpha_1, \dots, \alpha_n$ algebraic numbers in an algebraic number field of degree D. Let $b_1, \dots, b_n$ denote rational integers such that $\alpha_1^{b_1} \dots \alpha_n^{b_n}$ is not equal to* 1*. Let $A_1, \dots, A_n, B$ be real numbers with*

$$\log A_j \geq \max\left\{h(\alpha_j), \frac{1}{16\mathrm{e}^2 D^2}\right\}, \quad 1 \leq j \leq n,$$

and

$$B \geq \max\{|b_1|, \dots, |b_n|, 3\}.$$

If $n \geq 2$, then we have

$$\mathrm{v}_p(\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1) < (16\mathrm{e}D)^{2(n+1)} n^{5/2} (\log(2nD))^2 \, D^n \frac{p^D - 1}{(\log p)^2} \log A_1 \dots \log A_n \log B.$$

Theorem 2.9 allows us to improve slightly the dependence on p in Theorem 2.8; see also Theorem 12.3. Note that (as in Theorems 2.10 and 2.11, but unlike in Theorem 2.12 and in [443]) we do not assume that $\mathrm{v}_p(\alpha_j) = 0$ for $j = 1, \dots, n$.

The factor $(p^D - 1)$ in Theorem 2.9 and in Theorems 2.10 to 2.12 is ultimately due to the fact that the radius of convergence of the p-adic exponential function is finite, equal to $p^{-1/(p-1)}$. Removing it is a major open problem in the theory. This can be done under the rather restrictive assumption that $\mathrm{v}_p(\alpha_j - 1) > 0$ for $j = 1, \dots, n$; see [168, 169].

Theorem 2.9 should be compared with Theorem 2.2. We have exactly the same dependence on the parameters n, $\log A_1, \dots, \log A_n$, and B. A crucial point in Theorem 2.9 is the dependence on n, which is essential in the proofs of Theorems 8.2 and 8.3 towards the abc-conjecture. These proofs also require an estimate for $\mathrm{v}_p(\alpha_1^{b_1}\dots\alpha_n^{b_n}-1)$ with a (slightly) better dependence on p. For this reason, we quote the result stated on page 30 of [446].

Theorem 2.10. *We keep the notation of Theorem 2.9. If $n \geq 1$, then we have*

$$\mathrm{v}_p(\alpha_1^{b_1}\dots\alpha_n^{b_n}-1) < 12\,\frac{p^D-1}{\log p}\,\bigl(6(n+1)D\bigr)^{2(n+1)}\,\log(\mathrm{e}^5 nD) \\ \times\Bigl(\max\Bigl\{\frac{h(\alpha_1)}{\log p},1\Bigr\}\Bigr)\cdots\Bigl(\max\Bigl\{\frac{h(\alpha_n)}{\log p},1\Bigr\}\Bigr)\,\log B.$$

Yu [449] obtained an improvement of Theorem 2.10, with a better dependence on n, namely with n^n in place of $(n+1)^{2n}$. We refer to [449] for a precise statement.

The next statement, extracted from page 191 of Yu's paper [449], is the p-adic analogue of the main result of [25].

Theorem 2.11. *We keep the notation of Theorem 2.9. Let B_n be a real number such that*

$$B \geq B_n \geq |b_n|.$$

Assume that

$$\mathrm{v}_p(b_n) \leq \mathrm{v}_p(b_j), \quad j=1,\dots,n.$$

Let δ be a real number with $0<\delta\leq\frac{1}{2}$. Then, we have

$$\mathrm{v}_p(\alpha_1^{b_1}\dots\alpha_n^{b_n}-1) < (16\mathrm{e}D)^{2(n+1)}n^{3/2}\,(\log(2nD))^2\,D^n\,\frac{p^D-1}{(\log p)^2} \\ \times\max\Bigl\{(\log A_1)\cdots(\log A_n)(\log T),\,\frac{\delta B}{B_n c_0(n,D)}\Bigr\}, \quad (2.8)$$

where

$$T=\frac{B_n}{\delta}c_1(n,D)p^{(n+1)D}(\log A_1)\cdots(\log A_{n-1})$$

and

$$c_0(n,D)=(2D)^{2n+1}\log(2D)\log^3(3D), \quad c_1(n,D)=2\mathrm{e}^{(n+1)(6n+5)}D^{3n}\log(2D).$$

In particular, we get either

$$B\leq 2B_n(\log A_1)\cdots(\log A_n)\,c_0(n,D) \quad (2.9)$$

or

$$\mathrm{v}_p(\alpha_1^{b_1}\dots\alpha_n^{b_n}-1) < (16\mathrm{e}D)^{2(n+1)}n^{3/2}\,(\log(2nD))^2 D^n\,\frac{p^D}{(\log p)^2} \\ \times(\log A_1)\cdots(\log A_n)\,\max\Bigl\{1,\log\Bigl(\frac{c_1(n,D)p^{(n+1)D}B}{c_0(n,D)\log A_n}\Bigr)\Bigr\}. \quad (2.10)$$

The formulation of Theorem 2.11 looks complicated, but it essentially corresponds to the introduction of the parameter B' in Theorem 2.1 above. To get the second statement, we have selected

$$\delta_0 = \frac{(\log A_1) \cdots (\log A_n) B_n}{B} c_0(n, D)$$

and distinguished the two cases $\delta_0 \geq \frac{1}{2}$, which gives (2.9), and $\delta_0 < \frac{1}{2}$, which, by (2.8) with $\delta = \delta_0$, gives (2.10).

In the special case $b_n = 1$, the statements of Theorems 2.2 and 2.11 can be merged; see Theorem 3.2.8 of [183].

As for linear forms in complex logarithms, the case $n = 2$ is very important for applications. The next theorem reproduces one of the corollaries of the main result of [129].

THEOREM 2.12. *Let p be a prime number. Let α_1 and α_2 be multiplicatively independent algebraic numbers with $\mathrm{v}_p(\alpha_1) = \mathrm{v}_p(\alpha_2) = 0$. Set $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$. Let A_1 and A_2 be real numbers with*

$$\log A_j \geq \max\left\{h(\alpha_j), \frac{\log p}{D}\right\}, \quad j = 1, 2.$$

Let b_1 and b_2 be positive integers and set

$$\log B' = \max\left\{\log\left(\frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}\right) + \log\log p + 0.4, \frac{10 \log p}{D}, 10\right\}.$$

Then, we have the upper bound

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \leq \frac{24p(p^D - 1)}{(p-1)(\log p)^4} D^4 (\log A_1)(\log A_2) (\log B')^2. \tag{2.11}$$

The assumption that α_1 and α_2 are multiplicatively independent is not really restrictive for the applications and is useful to get small numerical values in (2.11). The assumption that α_1 and α_2 are p-adic units is not restrictive. Indeed, if only one among $\mathrm{v}_p(\alpha_1)$ and $\mathrm{v}_p(\alpha_2)$ is positive, then $\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) = 0$, while, if both of them are positive, then $\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2})$ is bounded from below by a positive real number times the minimum of b_1 and b_2.

A version of Theorem 2.12 (which is weaker only in terms of the numerical constants) is proved in this book; see Theorem 12.1.

Unlike Theorem 2.9, Theorem 2.12 cannot be applied to bound $\mathrm{v}_p(\alpha^b - 1)$ from above because of the assumption of multiplicative independence, but see Theorem 12.3.

Theorem 2.12 should be compared with Theorem 2.3. In particular, the numerical constant is very small and the quantity $\log B'$ also occurs squared.

We end this section with an improvement of Theorem 2.12 when α_1 and α_2 are rational numbers which are p-adically close to 1.

Let $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ be non-zero rational numbers. Theorem 2.13 below, originated in [109], provides an explicit upper bound for the p-adic valuation of the difference between integer powers of $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$.

We suppose that there exist a positive integer g and a real number E with $E > 1 + \frac{1}{p-1}$ and

$$\mathrm{v}_p\Big(\Big(\frac{x_1}{y_1}\Big)^g - 1\Big) \geq E, \tag{2.12}$$

and at least one of the two following conditions

$$\mathrm{v}_p\Big(\Big(\frac{x_2}{y_2}\Big)^g - 1\Big) \geq E \tag{2.13}$$

or

$$\mathrm{v}_p\Big(\Big(\frac{x_2}{y_2}\Big)^g - 1\Big) \geq 1 \quad \text{and} \quad \mathrm{v}_p(b_2) \leq \mathrm{v}_p(b_1) \tag{2.14}$$

is satisfied. For instance, if p is an odd prime number, then (2.12) and (2.13) hold with $g = 1$ if $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ are both congruent to 1 modulo p^2.

We stress that the assumption "(2.13) or (2.14) holds" is more restrictive than the assumption "$\mathrm{v}_p((\frac{x_2}{y_2})^g - 1) > 0$" made in [109]. However, it seems that the latter assumption is not sufficient to derive Theorem 2 from Theorem 1 in [109], a fact which has been overlooked in [109].

Theorem 2.13. *Let $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ be multiplicatively independent rational numbers. Let b_1, b_2 be positive integers. Assume that there exist a positive integer g and a real number E greater than $1 + \frac{1}{p-1}$ such that (2.12) holds, as well as (2.13) or (2.14). Let A_1, A_2 be real numbers with*

$$\log A_j \geq \max\{\log |x_j|, \log |y_j|, E \,\log p\}, \qquad j = 1, 2,$$

and put

$$\log B' = \max\Big\{\log\Big(\frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}\Big) + \log(E \,\log p) + 0.4, 6\, E \,\log p, 5\Big\}.$$

Then, we have the upper bound

$$\mathrm{v}_p\Big(\Big(\frac{x_1}{y_1}\Big)^{b_1} - \Big(\frac{x_2}{y_2}\Big)^{b_2}\Big) \leq \frac{36.1\, g}{E^3 \,(\log p)^4}(\log A_1)(\log A_2)(\log B')^2, \tag{2.15}$$

if p is odd or if $p = 2$ and $\mathrm{v}_2(\frac{x_2}{y_2} - 1) \geq 2$.

Observe that, if $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ are both congruent to 1 modulo p^3, then we can take $E = 3$ in Theorem 2.13 and the right hand side of (2.15) can be bounded independently of p.

A weaker version of Theorem 2.13 is proved in this book; see Theorem 12.2.

The parameter E in Theorem 2.13 should be compared with the parameter E in Theorems 2.1 and 2.4. Let us illustrate its importance with the following example taken from [117] (see also Exercise 6.11). Apply Theorem 2.13 with the prime number p to bound from above the p-adic valuation v of $(\frac{x}{y})^b - (1 + cp^k)$, for positive integers k, b, c, x, y, M with $k \geq 3$, $1 \leq c < p^{Mk}$, $x > p^k$, and $\gcd(p, b) = 1$. The latter assumption implies that, if $\mathrm{v} \geq 1$, then the p-adic valuations of $(\frac{x}{y})^b - 1$ and $\frac{x}{y} - 1$ are positive and equal. Consequently, p^k divides $\frac{x}{y} - 1$ and we apply Theorem 2.13 with $g = 1$, $A_1 = p^{(M+1)k}$, $A_2 = \max\{x, y\}$, and $E = k$ to get

$$\mathrm{v} \leq \frac{36.1}{\log p} \cdot \frac{\log A_1}{E(\log p)} (\log A_2)\,(6 + \log b)^2,$$

thus

$$\mathrm{v} \leq \frac{36.1(M+1)}{\log p}\,(\log A_2)\,(6 + \log b)^2.$$

This upper bound is independent of k. It considerably improves the upper bound given by (2.11) and can be viewed as an analogue of Theorem 2.5 (with $\frac{1}{\eta}$ replaced with $M+1$).

2.4. Notes

▷ Linear forms in one logarithm have been studied by Mignotte and Waldschmidt [300]. Let α be an algebraic number of degree $D \geq 2$ and of small height. In their lower bound for $|\alpha - 1|$ (that is, for $|\log \alpha|$), the dependence on D is much better than the one given by Liouville's inequality Theorem B.10; see also [134]. Amoroso [7] proved that these results are essentially sharp; see also [171]. A p-adic analogue has been worked out in [105].

▷ In the homogeneous rational case, a complete proof of Theorem 2.1 up to the dependence on n of the numerical constant has been given by Waldschmidt in [433]. Nesterenko [316] has written a detailed proof of Theorem 2.2 in the special case where $\alpha_1, \dots, \alpha_n$ are rational numbers. Aleksentsev [5] established an estimate of a similar strength as Theorem 2.2.

▷ There is a large gap between the size of the numerical constants in the best known lower bounds for linear forms in two and in three logarithms. For applications to Diophantine problems, it would be of greatest interest to improve the lower estimates for linear forms in three logarithms; see [298] for a step in this direction.

▷ Bugeaud [111] obtained lower bounds for linear forms in two logarithms and simultaneously for several p-adic valuations; see [52, 54, 111] for applications to Diophantine equations.

▷ Simultaneous linear forms in logarithms are discussed in Chapter 9.

Chapter 3
First applications

This chapter is principally devoted to Diophantine problems from which one can derive a linear form in complex logarithms in an almost obvious way, or, at least, in an easy way. We have listed them in increasing order of difficulty.

We postpone to Chapter 4 applications of the theory of linear forms in complex logarithms to classical families of Diophantine equations, including unit equations, Thue equations, elliptic equations, etc.

3.1. On the distance between powers of 2 and powers of 3

One of the simplest applications of the theory of linear forms in complex logarithms shows that the distance between a power of 2 and the power of 3 closest to it tends to infinity when the power of 2 tends to infinity. In addition, it provides us with an explicit lower bound for this distance. Of course, and this will be clear in Section 3.3, the integers 2 and 3 can be replaced by any pair of multiplicatively independent positive integers.

Theorem 3.1. *For all positive integers m and n, we have*

$$|2^m - 3^n| > 2^m \, (\mathrm{e}m)^{-8.4 \cdot 10^8}.$$

Proof. Let $n \geq 2$ be an integer and define m and m' by the conditions

$$2^{m'} < 3^n < 2^{m'+1} \quad \text{and} \quad |3^n - 2^m| = \min\{3^n - 2^{m'}, 2^{m'+1} - 3^n\}.$$

Then, m is equal to m' or to $m' + 1$ and

$$|2^m - 3^n| < 2^m, \quad (m-1)\log 2 < n \log 3 < (m+1)\log 2. \tag{3.1}$$

The problem of finding a lower bound for $|2^m - 3^n|$ clearly reduces to this case. Also, we have $m \geq n$. To show that 2^m cannot be too close to 3^n, it is sufficient to prove that the quantity

$$\Lambda := 3^n 2^{-m} - 1$$

is not too small in absolute value. Such a result is a direct consequence of Theorem 2.2, which, applied with $\alpha_1 = 3, A_1 = 3, \alpha_2 = 2, A_2 = 2$, gives that

$$\log |\Lambda| > -30^5 \cdot 2^{11/2} \cdot (\log 2)\,(\log 3)\,(\log \mathrm{e}m).$$

We conclude that

$$|3^n 2^{-m} - 1| > (\mathrm{e}m)^{-8.4\cdot 10^8},$$

and the theorem is established. □

As an application of Theorem 3.1, we list all the powers of 3 which differ from a power of 2 by at most 20. Our main auxiliary tool is the theory of continued fractions, briefly explained in Appendix A.

Theorem 3.2. *The only solutions in positive integers m, n with $n \geq 4$ to the inequality*

$$|2^m - 3^n| \leq 20 \tag{3.2}$$

are given by $|2^6 - 3^4| = 17$ *and* $|2^8 - 3^5| = 13$.

Proof. Let $n \geq 6$ and m be integers satisfying (3.2). Applying Theorem 3.1 to Inequality (3.2), we get

$$20 > 2^m \cdot (\mathrm{e}m)^{-8.4\cdot 10^8},$$

which implies

$$\log 20 > m \log 2 - 8.4 \cdot 10^8\,(1 + \log m),$$

giving $m < 4 \cdot 10^{10}$ and

$$n < \frac{(m+1)(\log 2)}{\log 3} < 3 \cdot 10^{10},$$

by (3.1). Since $|\log(1 + x)| \leq 2|x|$ for any real number x with $|x| < \frac{1}{2}$, the inequality $|2^m - 3^n| \leq 20$ implies

$$\left|\frac{\log 3}{\log 2} - \frac{m}{n}\right| \leq \frac{40}{n \log 2}\, 3^{-n}. \tag{3.3}$$

Observe that the right-hand side of (3.3) is less than $\frac{1}{2n^2}$, since $n \geq 6$. By Theorem A.2, the rational number $\frac{m}{n}$ is a convergent of the continued fraction expansion of $\xi := \frac{\log 3}{\log 2}$.

Furthermore, for $n < N := 3 \cdot 10^{10}$, the smallest value of $|m - n\xi|$ is obtained for the last convergent of the continued fraction expansion of ξ with denominator less than N. The computation of this expansion shows that

$$\left|\frac{\log 3}{\log 2} - \frac{m}{n}\right| > 9.6 \cdot 10^{-18}, \quad \text{for } 0 < n < 3 \cdot 10^{10}.$$

Comparing (3.3) with this estimate, we deduce that $n \leq 36$. A rapid verification in the range $6 \leq n \leq 36$ completes the proof that (3.2) has no solution with $n \geq 6$. □

3.2. Effective irrationality measures for quotients of logarithms of integers

Let a and b be multiplicatively independent positive rational numbers. It follows straightforwardly from the first assertion of Theorem 2.1 that the real number $\frac{\log a}{\log b}$ is transcendental and, by arguing as in the proof of Theorem 3.1, we show that it is not a Liouville number (see Definition A.6) and give an effective upper bound for its irrationality exponent (see Definition A.3).

Theorem 3.3. *Let a_1, a_2, b_1, b_2 be positive integers such that the rational numbers $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ are multiplicatively independent. Then, the effective irrationality exponent of the real number $(\log \frac{a_1}{a_2})/(\log \frac{b_1}{b_2})$ satisfies*

$$\mu_{\mathrm{eff}}\left(\frac{\log \frac{a_1}{a_2}}{\log \frac{b_1}{b_2}}\right) \ll (\log \max\{a_1, a_2\})\,(\log \max\{b_1, b_2\}).$$

A strengthening of Theorem 3.3 in the special case where $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ are rational numbers close to 1 is given in Section 5.1.

Proof. Let $\frac{p}{q}$ be a convergent to $(\log \frac{a_1}{a_2})/(\log \frac{b_1}{b_2})$ with $q \geq 2$. Since an irrational real number and its inverse have the same irrationality exponent, we can assume that $|\log \frac{a_1}{a_2}| < |\log \frac{b_1}{b_2}|$. It then follows from Theorem 2.1 (or from Theorem 2.2) that

$$\log\left|q \log \frac{a_1}{a_2} - p \log \frac{b_1}{b_2}\right| \gg -(\log \max\{a_1, a_2\})\,(\log \max\{b_1, b_2\})\,(\log q).$$

Thus, there exists an effectively computable, absolute real number C such that

$$\left|\frac{\log \frac{a_1}{a_2}}{\log \frac{b_1}{b_2}} - \frac{p}{q}\right| = \frac{|q \log \frac{a_1}{a_2} - p \log \frac{b_1}{b_2}|}{q \log \frac{b_1}{b_2}} \geq q^{-C(\log \max\{a_1,a_2\})\,(\log \max\{b_1,b_2\})}.$$

This proves the theorem. □

The fact that the dependence on B in Theorem 2.2 occurs through the factor $(\log B)$ and not through the factor $(\log B)^2$, as in Theorem 2.3, is crucial for the proof of Theorem 3.3.

3.3. On the distance between two integral S-units

For a finite set S of prime numbers, an integral S-unit is, by definition, an integer all of whose prime factors are in S. The following result extends Theorem 3.1. It was proved by Tijdeman [414] in 1973.

Theorem 3.4. *Let S denote a finite, non-empty set of prime numbers and $(x_j)_{j\geq 1}$ the increasing sequence of all positive integers whose prime factors belong to S. There exists an effectively computable real number C, depending only on S, such that*

$$x_{j+1} - x_j \geq x_j\,(\log 2x_j)^{-C}, \quad j \geq 1.$$

Proof. Write $S = \{q_1, \dots, q_s\}$, where $q_1, \dots, q_s$ are prime numbers and $q_1 < \cdots < q_s$. Let u, v with $3 \le u < v$ be two consecutive elements in the sequence $(x_j)_{j \ge 1}$ and write

$$u = \prod_{i=1}^{s} q_i^{u_i}, \quad v = \prod_{i=1}^{s} q_i^{v_i}.$$

Without any loss of generality, we can assume that $s \ge 2$, $v \le 2u$, and that u and v are coprime. Thus, for every $i = 1, \dots, s$, at least one of u_i, v_i is zero. Set

$$\Lambda := \prod_{i=1}^{s} q_i^{v_i - u_i} - 1 = \frac{v}{u} - 1.$$

Put $B = \max\{3, |v_1 - u_1|, \dots, |v_s - u_s|\}$ and observe that

$$2^{B/3} \le q_1^{B/3} \le v \le 2u. \tag{3.4}$$

It follows from Theorem 2.2 that

$$\log \Lambda \ge -30^{s+4}\, s^5 \Big(\prod_{i=1}^{s} \log q_i \Big) (\log \mathrm{e}B).$$

Combined with (3.4), this gives

$$\log\Big(\frac{v}{u} - 1\Big) \ge -30^{s+4}\, s^5 \Big(\prod_{i=1}^{s} \log q_i \Big) \log\Big(\frac{3\mathrm{e} \log(2u)}{\log 2} \Big).$$

Taking the exponential of both sides and multiplying by u, we get the assertion of the theorem. □

In view of the next result, established by Tijdeman [415] in 1974, Theorem 3.4 is essentially best possible.

Theorem 3.5. *Let P be an integer and S a finite set of at least two distinct prime numbers all being at most equal to P. Let $(x_j)_{j \ge 1}$ be the increasing sequence of all positive integers whose prime divisors belong to S. There exists an effectively computable real number C, depending only on P, such that*

$$x_{j+1} - x_j \le x_j \,(\log 2x_j)^{-C}, \quad j \ge 1.$$

It is an open problem of Erdős to establish that, for S being the set of all prime numbers less than P, Theorem 3.5 holds with a real number $C = C(P)$ which tends to infinity with P.

3.4. Effective irrationality measures for n-th roots of algebraic numbers

We have seen in Theorem 3.3 how the theory of linear forms in logarithms can be applied to give an effective upper bound for the irrationality exponent of certain transcendental real numbers. The next result addresses a special class of real algebraic numbers.

Theorem 3.6. *Let $n \ge 3$ be an integer and ξ a positive, real algebraic number. Then, the effective irrationality exponent of $\sqrt[n]{\xi}$ satisfies*

$$\mu_{\mathrm{eff}}(\sqrt[n]{\xi}) \ll_{\xi} \log n.$$

Furthermore, if a, b are integers with $1 \le b < a$, then we have

$$\mu_{\mathrm{eff}}(\sqrt[n]{a/b}) \ll (\log a)(\log n),$$

and, if $a \ge 2^n$, then we get

$$\mu_{\mathrm{eff}}(\sqrt[n]{a/b}) \le 11000 \log a. \tag{3.5}$$

When n is sufficiently large in terms of ξ, Theorem 3.6 improves the upper bound $\mu_{\mathrm{eff}}(\sqrt[n]{\xi}) \le n \deg(\xi)$, given by Liouville's Theorem A.5. It remains, however, very far from Roth's Theorem A.7, which asserts that $\mu(\sqrt[n]{\xi}) = 2$ but gives no information on $\mu_{\mathrm{eff}}(\sqrt[n]{\xi})$.

In Section 5.2 we considerably strengthen Theorem 3.6 when ξ is a rational number very close to 1.

Proof. Let $n \ge 3$ be an integer and ξ a positive, real algebraic number. Let $\frac{p}{q}$ be a convergent of $\sqrt[n]{\xi}$ with $q \ge 2$. Observe that

$$\left|\sqrt[n]{\xi} - \frac{p}{q}\right| \ge \frac{1}{2^n \max\{1, |\xi|\}} \left|\xi - \left(\frac{p}{q}\right)^n\right|.$$

It directly follows from Theorem 2.2 that

$$\log\left|\xi - \left(\frac{p}{q}\right)^n\right| > -C(\xi)(\log q)(\log n),$$

where $C(\xi)$ is an effectively computable real number which can be expressed in terms of the height and the degree of ξ. If ξ is the rational number $\frac{a}{b}$ with $1 \le b < a$, then $C(\xi)$ can be taken to be an absolute real number times $\log a$. This proves the first two statements of the theorem.

For large values of n, we obtain a stronger result (not only numerically) by applying Theorem 2.3. Indeed, if a, b are integers with $1 \le b < a$, it directly gives the lower bound

$$\log\left|n \log\left(\frac{p}{q}\right) - \log\left(\frac{a}{b}\right)\right| \ge -25.2(\log p)(\log a)\left(\max\left\{\log \frac{2n}{\log a} + 0.21, 20\right\}\right)^2,$$

if p is sufficiently large. From this and under the assumption $a \ge 2^n$, we deduce (3.5). □

3.5. On the greatest prime factor of values of integer polynomials

Let $f(X)$ be a non-zero integer polynomial with at least two distinct roots. Let n be an integer. Using the theory of linear forms in logarithms, Shorey and Tijdeman [374] were the first to give an effective lower bound for the greatest prime factor of $f(n)$ as n tends to infinity. In 1998 Tijdeman [418] noticed that, for the polynomial $X(X+1)$, the use of Theorem 2.2 allows us to improve the results of [374]. In his doctoral thesis, Haristoy [221] extended Tijdeman's result to an arbitrary polynomial $f(X)$. For an integer n, let denote by $P[n]$ its greatest prime factor with the convention that $P[0] = P[\pm 1] = 1$.

Theorem 3.7. *Let $f(X)$ be an integer polynomial with at least two distinct roots. Then, we have*

$$P[f(n)] \gg_f \log\log n \, \frac{\log\log\log n}{\log\log\log\log n}, \quad \textit{for } n \geq 10^7. \tag{3.6}$$

A result similar to Theorem 3.7 has been established in [217]; see also Chapter 8.

If we apply Theorem 2.1 (with a weaker dependence on the number of logarithms in the linear form than in Theorem 2.2) instead of Theorem 2.2, then we would get the weaker lower bound

$$P[f(n)] \gg_f \log\log n, \quad \text{for } n \geq 100,$$

which was obtained in [374].

Proof. To avoid technical complications, we treat only the case of the polynomial $X(X+1)$. For an integer n at least equal to 100, write

$$n(n+1) = p_1^{u_1} \ldots p_k^{u_k},$$

where $p_1 < p_2 < \cdots$ denotes the sequence of prime numbers in increasing order and the integers $u_1, \ldots, u_k$ are non-negative. There exist disjoint non-empty subsets I and J of $\{1, \ldots, k\}$ such that $I \cup J = \{1, \ldots, k\}$ and

$$n = \prod_{i \in I} p_i^{u_i}, \quad n+1 = \prod_{j \in J} p_j^{u_j}.$$

Then, there exist $\varepsilon_1, \ldots, \varepsilon_k$ in $\{\pm 1\}$ such that

$$\frac{n+1}{n} - 1 = |p_1^{\varepsilon_1 u_1} \ldots p_k^{\varepsilon_k u_k} - 1| = \frac{1}{n}\,. \tag{3.7}$$

Observe that

$$n+1 \geq 2^{u_j}, \quad j = 1, \ldots, k,$$

thus

$$\max_{1 \leq j \leq k} u_j \leq 2 \log n. \tag{3.8}$$

Since $p_j \ll j \log j$, for $j = 2, \ldots, k$, by Theorem D.2, we deduce from (3.8) and Theorems 2.2 and D.2 that there exist effectively computable, absolute real numbers c_1, c_2, c_3 such that

$$\begin{aligned}\log |p_1^{\varepsilon_1 u_1} \ldots p_k^{\varepsilon_k u_k} - 1| &\geq -c_1^k (\log p_1) \cdots (\log p_k)\, (\log\log n) \\ &\geq -c_2^{k \log\log k} \,(\log\log n),\end{aligned}$$

thus, by (3.7),

$$\log n \leq c_3^{k \log\log k} \, \log\log n\,.$$

By Theorem D.2, this implies that

$$p_k \gg k \log k \gg \log\log n \, \frac{\log\log\log n}{\log\log\log\log n},$$

as asserted.

The general case of an arbitrary monic, integer polynomial with distinct roots α and β rests on the same idea, but is technically more complicated. Let O_K denote the ring of integers of the algebraic number field $K := \mathbb{Q}(\alpha, \beta)$ and h its class number. Let n be an integer greater than $|\alpha|$ and $|\beta|$. Write the integer ideal $(n-\alpha)(n-\beta)O_K$ as a product of powers of prime ideals and raise this equality to the power h. Then, the quantity $(n-\alpha)^h(n-\beta)^{-h}$, which is equal to $1 + O(\frac{1}{n})$, can, with the help of Proposition C.5, be expressed as a product of powers of algebraic numbers in K whose heights are controlled. It then follows from Theorem 2.2 that this product cannot be too close to 1, hence the result. We leave the details to the reader. □

Let S be a finite non-empty set of prime numbers. For a non-zero integer n, write

$$[n]_S := \prod_{p \in S} |n|_p^{-1},$$

where $|\cdot|_p$ is the p-adic absolute value normalized such that $|p|_p^{-1} = p$. Said differently, $[n]_S$ is the greatest divisor of n, all of whose prime factors belong to S.

In 1984, Stewart [396] applied the theory of linear forms in logarithms to prove non-trivial effective upper bounds for $[n(n+1)\dots(n+k)]_S$, for any positive integer k. His result was later extended by Gross and Vincent [205] as follows; see also [122].

Theorem 3.8. *Let $f(X)$ be an integer polynomial with at least two distinct roots and S a finite, non-empty set of prime numbers. There exist effectively computable positive real numbers c_1 and c_2, depending only on $f(X)$ and S, such that, for every non-zero integer n which is not a root of $f(X)$, we have*

$$[f(n)]_S < c_1 |f(n)|^{1-c_2}.$$

Proof. To avoid technical complications, we treat only the case of the polynomial $X(X+1)$. We leave to the reader the details of the general case. Let n be an integer with $|n| \geq 2$. Write $S = \{q_1, \dots, q_s\}$, where s is the cardinality of S and $q_1 < \cdots < q_s$. Let $u_1, \dots, u_s$ be non-negative integers and a an integer coprime with $q_1 \cdots q_s$ such that

$$n(n+1) = q_1^{u_1} \dots q_s^{u_s} a.$$

There exist disjoint non-empty subsets I and J of $\{1, \dots, s\}$ such that $I \cup J = \{1, \dots, s\}$ and integers a', a'' such that $a = a'a''$ and

$$n = a' \prod_{i \in I} q_i^{u_i}, \quad n+1 = a'' \prod_{j \in J} q_j^{u_j}.$$

Then, there exist $\varepsilon_1, \dots, \varepsilon_s$ in $\{\pm 1\}$ such that

$$\frac{1}{n} = \frac{n+1}{n} - 1 = q_1^{\varepsilon_1 u_1} \dots q_s^{\varepsilon_s u_s} \frac{a''}{a'} - 1 =: \Lambda.$$

Noticing that $u_j \le 2 \log |n|$ for $j = 1, \ldots, s$, we deduce from Theorem 2.2 applied to Λ with the quantity B'' that there exists an effectively computable real number c_3 such that

$$-\log |n| \gg -c_3^s (\log q_1) \cdots (\log q_s)(\log \max\{|a'|, |a''|, 2\}) \log\Bigl(\frac{2(\log |n|)(\log q_s)}{\log \max\{|a'|, |a''|, 2\}}\Bigr).$$

This shows that there exists an effectively computable positive real number c_4, depending only on the set S, such that

$$\max\{|a'|, |a''|, 2\} \ge |n|^{c_4}.$$

If $|n| > 2^{1/c_4}$, then we get $a \ge \max\{|a'|, |a''|, 2\} \ge |n|^{c_4}$ and

$$[n(n+1)]_S = q_1^{u_1} \ldots q_s^{u_s} = \frac{n(n+1)}{a} \le \frac{n(n+1)}{|n|^{c_4}} \le (n(n+1))^{1-c_4/3},$$

which gives the desired result.

We now explain how a suitable version of Theorem 3.8 with explicit values for c_1 and c_2 implies Theorem 3.7. Observe that, setting $C := c_3^s (\log q_1) \cdots (\log q_s)$, an admissible value for c_4 is given by

$$c_4 = c_5 C^{-1} (\log(C \log q_s))^{-1},$$

for some suitable absolute real number c_5. If S is the set composed of the first s prime numbers, then it follows from Theorem D.2 that c_4 exceeds $c_6^{-s \log \log s}$ for some absolute real number c_6. If $P[n(n+1)] = p_s$, then $\max\{|a'|, |a''|, 2\} = 2$ and $|n|^{c_4} \le 2$, thus,

$$\log |n| \le 2 c_6^{s \log \log s}.$$

Combined with Theorem D.2, this gives

$$P[n(n+1)] \gg \log \log n \, \frac{\log \log \log n}{\log \log \log \log n},$$

and we recover Theorem 3.7. □

3.6. On the greatest prime factor of terms of linear recurrence sequences

Let k be a positive integer, $a_1, \ldots, a_k$ and $u_0, \ldots, u_{k-1}$ be integers such that a_k is non-zero and $u_0, \ldots, u_{k-1}$ are not all zero. Put

$$u_n = a_1 u_{n-1} + \cdots + a_k u_{n-k}, \quad \text{for } n \ge k.$$

The sequence $(u_n)_{n \ge 0}$ is a linear recurrence sequence of integers of order k. Its companion (or, characteristic) polynomial

$$G(z) := z^k - a_1 z^{k-1} - \cdots - a_k$$

factors as

$$G(z) = \prod_{i=1}^{t} (z - \alpha_i)^{\ell_i},$$

where $\alpha_1, \ldots, \alpha_t$ are distinct algebraic numbers, ordered in such a way that $|\alpha_1| \geq \cdots \geq |\alpha_t|$, and $\ell_1, \ldots, \ell_t$ are positive integers. Then, (see e.g. [179] or Chapter C of [376]) there exist polynomials $f_1(X), \ldots, f_t(X)$ of degrees less than $\ell_1, \ldots, \ell_t$, respectively, and with coefficients in $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$, such that

$$u_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n, \quad \text{for } n \geq 0.$$

The recurrence sequence $(u_n)_{n\geq 0}$ is said to be degenerate if there are integers i, j with $1 \leq i < j \leq t$ such that $\frac{\alpha_i}{\alpha_j}$ is a root of unity. We say that $(u_n)_{n\geq 0}$ has a dominant root if $|\alpha_1| > |\alpha_2|$ and $f_1(X)$ is not the zero polynomial.

The next result was established in [399]; see also [395].

Theorem 3.9. *Let* $\mathbf{u} := (u_n)_{n\geq 0}$ *be a recurrence sequence of integers given by*

$$u_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n, \quad \textit{for } n \geq 0,$$

and having a dominant root α_1*. For any integer* n *greater than* 100 *and such that* u_n *is not equal to* $f_1(n)\alpha_1^n$*, the greatest prime factor of* u_n *satisfies*

$$P[u_n] \gg_{\mathbf{u}} \log n \, \frac{\log\log n}{\log\log\log n}. \tag{3.9}$$

Proof. We establish a slightly more general result. We consider a sequence of non-zero integers $\mathbf{v} := (v_n)_{n\geq 0}$ with the property that there are θ in $(0, 1)$ and a positive real number C such that

$$|v_n - f(n)\alpha^n| \leq C\,|\alpha|^{\theta n}, \quad n \geq 0,$$

where $f(X)$ is a non-zero polynomial whose coefficients are algebraic numbers and α is an algebraic number with $|\alpha| > 1$. Clearly, a recurrence sequence having a dominant root α has the above property.

Let $p_1, p_2, \ldots$ be the sequence of prime numbers in increasing order. Let n be a positive integer such that $f(n)$ is non-zero and $v_n \neq f(n)\alpha^n$. Assume that the greatest prime factor of v_n is equal to p_k, that is, assume that

$$v_n = p_1^{r_1} \cdots p_k^{r_k},$$

where $r_1, \ldots, r_k$ are non-negative integers and $r_k \geq 1$. Then, we have

$$\Lambda := |p_1^{r_1} \cdots p_k^{r_k} f(n)^{-1}\alpha^{-n} - 1| \leq C|f(n)|^{-1}\,|\alpha|^{(\theta-1)n},$$

and, since $\theta < 1$, we get

$$\log\Lambda \ll_{\mathbf{v}} (-n).$$

As $v_n \neq f(n)\alpha^n$, the quantity Λ is non-zero and Theorem 2.2 implies that

$$\log\Lambda \gg_{\mathbf{v}} -c_1^k\,(\log p_1)\cdots(\log p_k)\,(\log n)^2,$$

where c_1 is an effectively computable, positive, absolute real number. Comparing both estimates for $\log \Lambda$, we obtain that

$$n \ll_{\mathbf{v}} (c_1 \log p_k)^k (\log n)^2,$$

thus, by Theorem D.2,

$$\log n \ll_{\mathbf{v}} \frac{p_k}{\log p_k} \log\log p_k.$$

This implies that

$$P[v_n] = p_k \gg_{\mathbf{v}} \log n \frac{\log\log n}{\log\log\log n},$$

and the theorem is established. □

The lower bound for $P[u_n]$ in (3.9) is of similar strength as the one for $P[f(n)]$ in Theorem 3.7, since $|u_n|$ grows exponentially fast in n. Both proofs show that $\gg_f$ in (3.6) and $\gg_{\mathbf{u}}$ in (3.9) can be replaced by $\geq (1-\varepsilon)$, for any positive ε and any sufficiently large integer n.

3.7. Perfect powers in linear recurrence sequences

We continue the study of arithmetical properties of linear recurrence sequences of integers having a dominant root and show that no term of such a sequence can be a very large power of an integer greater than one.

THEOREM 3.10. *Let $\mathbf{u} := (u_n)_{n\geq 0}$ be a recurrence sequence of integers given by*

$$u_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n, \quad \text{for } n \geq 0,$$

and having a dominant root α_1. Assume that α_1 is a simple root, that is, the polynomial $f_1(X)$ is equal to a non-zero algebraic number f_1. Then, the equation

$$u_n = y^q,$$

in integers n, y, q with q a prime number, $|y| \geq 2$, and $u_n \neq f_1\alpha_1^n$, implies that

$$q \ll_{\mathbf{u}} 1.$$

Theorem 3.10 was proved in [372]; see also [190, 325]. More can be said in the case of binary recurrence sequences, see Section 6.9.

Proof. We establish a slightly more general result. We consider a sequence of non-zero integers $\mathbf{v} := (v_n)_{n\geq 0}$ with the property that there are θ in $(0,1)$ and a positive real number C such that

$$|v_n - f\alpha^n| \leq C\,|\alpha|^{\theta n}, \quad n \geq 0,$$

where f is a non-zero algebraic number and α is an algebraic number with $|\alpha| > 1$.

Let n, y, q with q a prime number be such that $v_n = y^q$, $|y| \geq 2$, and $v_n \neq f\alpha^n$. Then, we have

$$|f^{-1}\alpha^{-n}y^q - 1| \leq \frac{C}{|f|}\,|\alpha|^{(\theta-1)n}. \tag{3.10}$$

There exist integers k and r such that $n = kq + r$ with $|r| \leq \frac{q}{2}$. Rewriting (3.10) as

$$\Lambda := \left| f^{-1}\left(\frac{y}{\alpha^k}\right)^q \alpha^{-r} - 1 \right| \leq \frac{C}{|f|} |\alpha|^{(\theta-1)n},$$

we observe that

$$\log \Lambda \ll_{\mathbf{v}} (-n). \tag{3.11}$$

By Theorem B.5, the height of $\frac{\alpha^k}{y}$ is bounded from above by the sum of $\log |y|$ and k times the height of α. Since

$$q \log |y| \ll_{\mathbf{v}} n \leq (k+1)q \quad \text{and} \quad \frac{kq}{2} \leq n \ll_{\mathbf{v}} q \log |y|, \tag{3.12}$$

we get that $h(\alpha^k/y) \ll_{\mathbf{v}} \log |y|$. It then follows from Theorem 2.2 that

$$\log \Lambda \gg_{\mathbf{v}} -(\log |y|)(\log q),$$

which, combined with (3.11) and (3.12), gives

$$q \log |y| \ll_{\mathbf{v}} n \ll_{\mathbf{v}} (\log |y|)(\log q),$$

and we get $q \ll_{\mathbf{v}} 1$. This proves the theorem. □

We point out a very special case of Theorem 3.10.

Corollary 3.11. *Let α and β be algebraic integers such that $\alpha + \beta$, $\alpha\beta$ are rational integers and $\alpha > |\beta|$. Then, the equation*

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = y^q \quad (\textit{resp., } \alpha^n + \beta^n = y^q), \tag{3.13}$$

in integers n, y, q with $|y| \geq 2$ and q a prime number, implies that

$$q \ll_{\alpha,\beta} 1.$$

Let us discuss a celebrated example of resolution of equations of the form (3.13), namely the determination of all the perfect powers among the Fibonacci and Lucas numbers. Set $\gamma = \frac{1+\sqrt{5}}{2}$ and observe that $-\gamma^{-1} = \frac{1-\sqrt{5}}{2}$. Let the integer sequences $(F_n)_{n\geq 0}$ and $(L_n)_{n\geq 0}$ be defined respectively by

$$F_n = \frac{\gamma^n - (-\gamma^{-1})^n}{\gamma - (-\gamma^{-1})}, \quad L_n = \gamma^n + (-\gamma^{-1})^n,$$

so that the first elements of the Fibonacci sequence $(F_n)_{n\geq 0}$ and of the Lucas sequence $(L_n)_{n\geq 0}$ are given by

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots$$

and

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots,$$

respectively. The Fibonacci sequence is an emblematic example of a Lucas–Lehmer sequence (see Section 7.2). The following result has been established in [137].

Theorem 3.12. *The only perfect powers in the sequence* $(F_n)_{n\geq 0}$ *are* 0*,* 1*,* 8*, and* 144*. The only perfect powers in the sequence* $(L_n)_{n\geq 0}$ *are* 1 *and* 4*.*

Outline of the proof. The complete proof is much too involved to be included in the present textbook, however, it is appropriate to discuss the main steps of the proof of the first assertion. The lists of squares and cubes in the Fibonacci sequence were obtained by Ljunggren [265, 266] and London and Finkelstein [268], respectively. Their proofs are elementary, in the sense that they do not rest on the theory of linear forms in logarithms. The equation $F_n = y^5$ was solved by Pethő [324], by using a linear form in logarithms and congruence conditions; see [137] for additional references.

Let $n \geq 13$ be an integer, $q \geq 7$ a prime number, and suppose that $F_n = y^q$ for some integer $y \geq 2$. Then, noticing that $\gamma + \gamma^{-1} = \sqrt{5}$ and proceeding exactly as in the proof of Theorem 3.10, we derive that there exist integers k and r such that $n = kq + r$ with $|r| \leq \frac{q}{2}$ and

$$\Lambda := \left|\sqrt{5}\Big(\frac{y}{\gamma^k}\Big)^q \gamma^{-r} - 1\right| \ll y^{-2q}.$$

The quantity Λ is a linear form in three logarithms. Since $h(y/\gamma^k) \ll \log y$ it follows from Theorem 2.2 that

$$\log \Lambda \gg -(\log y)\,(\log q),$$

and, comparing both estimates, we deduce an upper bound for the exponent q. Actually, a special estimate for linear forms in three logarithms proved in [137] (see also [298]) implies the sharper upper bound $q < 2 \cdot 10^8$, a range which is suitable for computer calculations. Then, a sieve performed by using the “modular method” allows us to prove that $r = \pm 1$, for any prime number q between 7 and $2 \cdot 10^8$. This shows that our linear form in three logarithms can be written as a linear form in only two logarithms, namely

$$\Lambda = \left|\Big(\frac{y}{\gamma^k}\Big)^q (\gamma^{\pm 1}\sqrt{5}) - 1\right|.$$

An application of Theorem 2.3 (actually, of the main result of [254]) now leads to the much better upper bound $q \leq 733$. It then remains to treat a reasonably small number of equations. A second sieve, again performed by using the “modular method”, allows us to prove that, for any prime number q between 7 and 733, the index n must be very large. To get a contradiction, we have to bound n from above. To do this, observe that the Fibonacci and Lucas numbers are linked by the relation

$$5F_m^2 - L_m^2 = 4, \quad \text{for } m \geq 1 \text{ odd}.$$

Since we have assumed that $F_n = y^q$, this implies that the equation

$$X^2 + 4 = 5Y^{2q}$$

has a solution in positive integers X, Y with $Y > 1$, given by $(X, Y) = (L_n, y)$. This equation is similar to the equations considered in Section 4.6 below, with, however, an important difference. Namely, since

$$(-1)^2 + 4 = 1 + 4 = 5 = 5 \cdot 1^{2q},$$

it has always solutions, regardless of the prime number q. At present, we are not able to solve it completely, but we can explicitly bound the absolute values of its solutions. The authors of [137] have proceed as follows.

Let X, Y be positive integers with $Y \geq 2$ and $X^2 + 4 = 5Y^{2q}$. By factoring over $\mathbb{Z}[\mathrm{i}]$ the left-hand side of this equality, we deduce the existence of integers a and b with $a^2 + b^2 = Y^2$ and

$$\pm 4\mathrm{i} = (2 + \mathrm{i})(a + \mathrm{i}b)^q - (2 - \mathrm{i})(a - \mathrm{i}b)^q.$$

Dividing both members of the inequality by 2i, we get

$$\begin{aligned}\pm 2 = 2 \sum_{k=0}^{[q/2]} \binom{q}{2k} a^{2k} \, (-1)^{(q-2k-1)/2} \, b^{q-2k} \\ + \sum_{k=0}^{[q/2]} \binom{q}{2k+1} a^{2k+1} \, (-1)^{(q-2k-1)/2} \, b^{q-2k-1}.\end{aligned}$$

We infer that a is even. Consequently, $(b, \frac{a}{2})$ is an integer solution of the Diophantine equation

$$\sum_{k=0}^{q} (-4)^{\lfloor (q-k)/2 \rfloor} \binom{q}{k} Z^k \, T^{q-k} = \pm 1,$$

in integer unknowns Z and T. We recognize a Thue equation of degree q. As explained in Section 4.3 below, the theory of linear form in logarithms allows us to bound from above the absolute values of its solutions. Thus, we get an explicit upper bound for $|a|$ and $|b|$, hence for Y. This in turn implies an explicit upper bound for the index n. Since this bound is smaller than the bound obtained via the second sieve, we have reached a contradiction. Consequently, there are no q-th powers greater than 1 in the Fibonacci sequence, where $q \geq 7$ is a prime number. This completes the outline of the proof of the theorem. □

3.8. Simultaneous Pellian equations and Diophantine quadruples

Let $a \geq 2$ be an integer which is not a perfect square and u a non-zero integer. By Theorem C.2, the Pellian equation

$$x^2 - ay^2 = u,$$

in integers x, y, has either no solutions or infinitely many. This motivates the study of systems of two Pellian equations having an unknown in common. Let $b \geq 2$ be an integer which is not a perfect square, distinct from a, and v a non-zero integer. We consider the systems

$$x^2 - ay^2 = u, \qquad x^2 - bz^2 = v, \qquad \text{in integers } x, y, z, \tag{3.14}$$

$$x^2 - ay^2 = u, \qquad y^2 - bz^2 = v, \qquad \text{in integers } x, y, z, \tag{3.15}$$

and

$$x^2 - ay^2 = u, \qquad z^2 - by^2 = v, \qquad \text{in integers } x, y, z.$$

Solving any of these systems amounts to determine the common values of two binary recurrence sequences of integers; see [44] and the references quoted therein.

Theorem 3.13. *Let a, b be positive integers which are not perfect squares. Let u, v be non-zero integers such that $av \neq bu$. Then, all the solutions in positive integers x, y, z to the system of simultaneous Pellian equations*

$$x^2 - ay^2 = u, \quad z^2 - by^2 = v \tag{3.16}$$

satisfy

$$\max\{x, y, z\} \ll_{a,b,u,v} 1.$$

A similar result holds for the systems (3.14) and (3.15) of simultaneous Pellian equations.

Let x, y, z be integers satisfying (3.16). Setting $w = xz$, we derive the equation

$$w^2 = (ay^2 + u)(by^2 + v),$$

which belongs to a general family of Diophantine equations treated in Theorem 4.7. Observe that the polynomial $(aX + u)(bX + v)$ is not a square when $av \neq bu$.

Proof. Let ε and η be the fundamental units (see Definition C.3) of the rings of integers of the fields $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, respectively. Let x, y, and z be positive integers satisfying (3.16). Since the norm over $\mathbb{Q}$ of $x + y\sqrt{a}$ (*resp.*, $z + y\sqrt{b}$) is u (*resp.*, v), it follows from Proposition C.5 that there exist nonnegative integers m, n and algebraic numbers α in $\mathbb{Q}(\sqrt{a})$ and β in $\mathbb{Q}(\sqrt{b})$, with $h(\alpha) \ll_{a,u} 1$ and $h(\beta) \ll_{b,v} 1$, such that

$$x + y\sqrt{a} = \alpha\varepsilon^m \quad \text{and} \quad z + y\sqrt{b} = \beta\eta^n.$$

Consequently, we have

$$2y\sqrt{a} = \alpha\varepsilon^m - \alpha^\sigma(\varepsilon^\sigma)^m$$

and

$$2y\sqrt{b} = \beta\eta^n - \beta^\sigma(\eta^\sigma)^n,$$

where the superscript $\cdot^\sigma$ denotes the Galois conjugacy. Since $|\varepsilon^\sigma| = \varepsilon^{-1}$ and $|\eta^\sigma| = \eta^{-1}$, we get

$$\Lambda := |\alpha\beta^{-1}\varepsilon^m\eta^{-n} - 1| \ll_{a,b,u,v} (\varepsilon^{-m} + \eta^{-n}). \tag{3.17}$$

As pointed out at the end of Section C.1, the units ε and η are at least equal to the Golden Ratio, thus it follows from (3.17) and Theorem 2.2 that

$$-\log\max\{m, n\} \ll_{a,b,u,v} \log\Lambda \ll_{a,b,u,v} (-\min\{m, n\}).$$

Since $\min\{m, n\} \gg_{a,b,u,v} \max\{m, n\}$, this shows that m and n are bounded by an effectively computable real number depending on a, b, u, and v. Consequently, we have proved that $\max\{x, y, z\} \ll_{a,b,u,v} 1$. □

The Greek mathematician Diophantus observed that the rational numbers $\frac{1}{16}$, $\frac{33}{16}$, $\frac{17}{4}$, and $\frac{105}{16}$ have the following property: the product of any two of them increased by 1 is a square of a rational number. Later, Fermat noted that the set $\{1, 3, 8, 120\}$ shares the same property. For $m \geq 3$, we call a Diophantine m-tuple any set of m positive integers $a_1, \ldots, a_m$ such that $a_i a_j + 1$ is a perfect square whenever $1 \leq i < j \leq m$. It was known already to Euler that there are infinitely many Diophantine quadruples. Baker and Davenport [35] established that 120 is the unique positive integer t such that $\{1, 3, 8, t\}$ is a Diophantine quadruple. Among the broad literature on that topic, let us mention that Dujella [172] proved that there exist no Diophantine sextuple and that every element of a Diophantine quintuple is less than $10^{10^{26}}$. The question of the non-existence of a Diophantine quintuple remains a very challenging open problem.

The proof of the result of Baker and Davenport [35] reduces to the complete resolution of a system of simultaneous Pellian equations.

Theorem 3.14. *The only positive integer t such that $\{1, 3, 8, t\}$ is a Diophantine quadruple is* 120.

A key ingredient in the proof of Theorem 3.14 is Lemma 3.15, usually called the Baker–Davenport lemma. Throughout, $\| \cdot \|$ denotes the distance to the nearest integer.

Lemma 3.15. *Let θ and β be real numbers. Let $A > 0$ and $C > 1$ be real numbers. Let $K \geq 6$, $M \geq 1$, p, q be integers satisfying*

$$1 \leq q \leq KM, \quad |q\theta - p| < \frac{2}{KM}. \tag{3.18}$$

If

$$\|q\beta\| \geq \frac{3}{K}, \tag{3.19}$$

then the inequality

$$|m\theta - n + \beta| < AC^{-m} \tag{3.20}$$

has no solutions in integers m, n, with

$$\frac{\log AK^2M}{\log C} < m < M. \tag{3.21}$$

Proof. Let m, n be integers and assume that m satisfies (3.21). Setting $\phi := q\theta - p$ and multiplying (3.20) by q, we get

$$|(pm - nq) + m\phi + \beta q| = |(q\theta)m - nq + \beta q| < AqC^{-m}. \tag{3.22}$$

Since $m < M$, we have $|m\phi| < \frac{2}{K}$, while $m > (\log AK^2M)/(\log C)$ implies that

$$AqC^{-m} < \frac{Aq}{AK^2M} \leq \frac{1}{K}.$$

By (3.22), we deduce that

$$\|q\beta\| < |m\phi| + AqC^{-m} < \frac{1}{K} + \frac{2}{K} \leq \frac{3}{K},$$

a contradiction with (3.19). □

Outline of the proof of Theorem 3.14. Let t be a positive integer such that $\{1, 3, 8, t\}$ is a Diophantine quadruple. Then, there exist positive integers x, y, z such that

$$t + 1 = x^2, \quad 3t + 1 = y^2, \quad 8t + 1 = z^2.$$

In particular, we get

$$3x^2 - y^2 = 2 \quad \text{and} \quad 8x^2 - z^2 = 7.$$

Classical results (see Section C.1) tell us that there exist non-negative integers m, n and ε in $\{\pm 1\}$ such that the positive integers x, y, z are given by

$$y + x\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^m$$

and

$$z + x\sqrt{8} = (\varepsilon + \sqrt{8})(3 + \sqrt{8})^n.$$

Consequently, we arrive at

$$\begin{aligned} 2x &= \frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m + \frac{\sqrt{3}-1}{\sqrt{3}}(2+\sqrt{3})^{-m} \\ &= \frac{\varepsilon+\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^n + \frac{\sqrt{8}-\varepsilon}{\sqrt{8}}(3+\sqrt{8})^{-n}. \end{aligned}$$

Thus, assuming $m \geq 3$, we get $n < m$ and, after some calculation,

$$0 < m \log(2+\sqrt{3}) - n \log(3+\sqrt{8}) + \log \frac{(1+\sqrt{3})\sqrt{8}}{(\varepsilon+\sqrt{8})\sqrt{3}} < \frac{2}{(2+\sqrt{3})^{2m}}. \tag{3.23}$$

Combined with Theorem 2.2, we deduce an upper bound for m. Using Theorem 1.9, Baker and Davenport obtained the upper bound

$$m < 10^{487}. \tag{3.24}$$

Furthermore, dividing (3.23) by $\log(3+\sqrt{8})$, we get the inequality

$$|m\theta_0 - n + \beta_0| < A_0 C_0^{-m}, \tag{3.25}$$

where

$$\theta_0 := \frac{\log(2+\sqrt{3})}{\log(3+\sqrt{8})}, \quad \beta_0 := \frac{1}{\log(3+\sqrt{8})} \log \frac{(1+\sqrt{3})\sqrt{8}}{(\varepsilon+\sqrt{8})\sqrt{3}},$$

and

$$A_0 := \frac{2}{\log(3+\sqrt{8})}, \quad C_0 := (2+\sqrt{3})^2.$$

Classical results from metrical number theory (see e.g. Theorem II in Chapter VII of [144]) assert that, for almost all (with respect to the Lebesgue measure) pairs (θ', β') of real numbers and for every positive real number ε, the inequality

$$|m\theta' - n + \beta'| < m^{-1-\varepsilon}$$

has only finitely many solutions in integers m, n. Thus, it is rather unlikely that there exist large integers m, n satisfying (3.25).

Since β_0 is non-zero, we cannot use continued fractions as in the proof of Theorem 3.2. However, Lemma 3.15 gives us a numerical method to reduce the bound (3.24). We proceed as follows. Using the theory of continued fractions (see Appendix A), we find suitable integers p, q, K, M with $M > M_0$ which fulfill the assumptions of Lemma 3.15 applied with θ_0, β_0, A_0, and C_0. For instance, one can select for $\frac{p}{q}$ a convergent to θ, the factor 2 in the numerator in (3.18) being there to allow some more flexibility.

Baker and Davenport applied Lemma 3.15 with $M = 10^{487}$ and $K = 10^{33}$. They took for $\frac{p}{q}$ the last convergent with $q \le 10^{520}$ to the rational number θ_1, whose 1040 first decimals coincide with those of θ_0 and whose other decimals are 0. It then follows that there are no solutions with $m \ge 500$. These small values of m can then be treated directly, or we can again apply Lemma 3.15 to refine the estimate $m \le 499$, before treating directly the remaining values of m. □

3.9. On the representation of integers in distinct bases

Let a and b be integers at least equal to 2. In 1973, Senge and Straus [363] proved that the number of integers, the sum of whose digits in each of the bases a and b lies below a fixed bound, is finite if and only if a and b are multiplicatively independent. Their proof rests on the Roth Theorem A.7 and, hence, is ineffective. Using the theory of linear forms in logarithms, Stewart [394] succeeded in establishing an effective version of Senge and Straus' theorem. He showed that if a and b are multiplicatively independent, then, for every $c \ge 1$, each integer $m > 25$ whose sum of digits in base a as well as in base b is bounded by c satisfies

$$\frac{\log\log m}{\log\log\log m + c_1} < 2c + 1, \tag{3.26}$$

where c_1 is a positive real number which is effectively computable in terms of a and b only; see also [272, 295].

Besides the number of non-zero digits in the representation of an integer m, we may also estimate the number of blocks composed of the same digit in this representation. This was first considered by Blecksmith, Filaseta, and Nicol [79], who proved that, for multiplicatively independent positive integers a and b, we have

$$\lim_{n \to +\infty} BC(a^n, b) = +\infty,$$

where $BC(m, b)$ stands for the number of times that a digit different from the previous one is read in the b-ary representation of the positive integer m. Their result was subsequently quantified by Barat, Tichy, and Tijdeman [40], who, under the same assumption, showed that there are effectively computable real numbers c_2, n_0, depending only on a and b, such that

$$BC(a^n, b) \ge c_2 \frac{\log n}{\log\log n}, \quad \text{for } n > n_0.$$

Their proof is similar to that of Stewart [394]. We note that if m has at most k non-zero digits in its b-ary representation, then $BC(m, b)$ does not exceed $2k$. However, the converse is not true, since a number m for which $BC(m, b)$ is small may have many non-zero digits in its b-ary representation. The next statement, whose proof follows Stewart's arguments, extends (3.26).

Theorem 3.16. *Let a and b be multiplicatively independent integers. Then we have*

$$BC(m,a) + BC(m,b) \geq \frac{\log\log m}{\log\log\log m + C}, \tag{3.27}$$

for $m > 25$, where C is a positive number which is effectively computable in terms of a and b only.

Proof. Let $m > a^4$ be an integer and let its a-ary representation be given by

$$m = a_h a^h + \cdots + a_1 a + a_0,$$

with $a_h \neq 0$. Define the integers $n_1 < n_2 < \cdots < n_r$ by $n_r = h$, $a_0 = \cdots = a_{n_1}$, $a_{n_1} \neq a_{n_1+1}$ and $a_{n_j+1} = \cdots = a_{n_{j+1}}$, $a_{n_{j+1}} \neq a_{n_{j+1}+1}$ for $j \geq 1$, until we reach a_h. Then, observe that

$$\begin{aligned} m &= a_{n_1}\frac{a^{n_1+1}-1}{a-1} + a_{n_2}a^{n_1+1}\frac{a^{n_2-n_1}-1}{a-1} + \cdots + a_{n_r}a^{n_{r-1}+1}\frac{a^{n_r-n_{r-1}}-1}{a-1} \\ &= -\frac{a_{n_1}}{a-1} + \frac{a_{n_1}-a_{n_2}}{a-1}a^{n_1+1} + \frac{a_{n_2}-a_{n_3}}{a-1}a^{n_2+1} + \cdots + \frac{a_{n_r}}{a-1}a^{n_r+1}. \end{aligned}$$

Likewise, if

$$m = b_k b^k + \cdots + b_1 b + b_0,$$

where $b_k \neq 0$, denotes the b-ary representation of m, we define the integers $\ell_1 < \ell_2 < \cdots < \ell_t$ by $\ell_t = k$, $b_0 = \cdots = b_{\ell_1}$, $b_{\ell_1} \neq b_{\ell_1+1}$ and $b_{\ell_j+1} = \cdots = b_{\ell_{j+1}}$, $b_{\ell_{j+1}} \neq b_{\ell_{j+1}+1}$ for $j \geq 1$, until we reach b_k. We have

$$m = -\frac{b_{\ell_1}}{b-1} + \frac{b_{\ell_1}-b_{\ell_2}}{b-1}b^{\ell_1+1} + \frac{b_{\ell_2}-b_{\ell_3}}{b-1}b^{\ell_2+1} + \cdots + \frac{b_{\ell_t}}{b-1}b^{\ell_t+1}.$$

Put $\theta = c_1 \log\log m$ for a real number $c_1 \geq 3$ which depends on a and b and will be fixed later. Since m exceeds e^{e}, we have $\theta \geq 3$. Define k to be the integer satisfying

$$\theta^k \leq \frac{\log m}{4\log a} < \theta^{k+1}, \tag{3.28}$$

and put

$$I_1 = (1,\theta], I_2 = (\theta,\theta^2], \ldots, I_k = (\theta^{k-1},\theta^k].$$

Assume that m is large enough to satisfy

$$\log m \geq 4c_1(\log a)(\log\log m). \tag{3.29}$$

This ensures that $k \geq 1$.

If each of the intervals $I_1, \ldots, I_k$ contains at least one term of the form $n_r - n_u$ with $1 \leq u \leq r-1$ or of the form $\ell_t - \ell_v$ with $1 \leq v \leq t-1$, then

$$BC(m,a) + BC(m,b) \geq r + t - 2 \geq k. \tag{3.30}$$

However, it follows from (3.28) that

$$(k+1)\log\theta > \log\log m - \log(4\log a).$$

Combined with (3.30) and our choice of θ, this gives

$$BC(m,a) + BC(m,b) \ge \frac{\log\log m - \log(4\log a)}{\log\log\log m + \log c_1} - 1,$$

which implies (3.27) for a suitable C.

Therefore, we may assume that there is an integer s, with $1 \le s \le k$, for which the interval I_s contains no term of the form $n_r - n_u$ with $1 \le u \le r-1$ or of the form $\ell_t - \ell_v$ with $1 \le v \le t-1$. Define the integers p and q by the inequalities

$$n_r - n_p \le \theta^{s-1} \quad \text{and} \quad n_r - n_{p-1} > \theta^s,$$

and

$$\ell_t - \ell_q \le \theta^{s-1} \quad \text{and} \quad \ell_t - \ell_{q-1} > \theta^s,$$

with the convention that $n_0 = \ell_0 = 0$. Then, setting

$$A_1 = a_{n_r} a^{n_r+1-n_p} + (a_{n_{r-1}} - a_{n_r}) a^{n_{r-1}+1-n_p} + \cdots + (a_{n_p} - a_{n_{p+1}}) a$$

and

$$A_2 = (a_{n_{p-1}} - a_{n_p}) a^{n_{p-1}+1} + (a_{n_{p-2}} - a_{n_{p-1}}) a^{n_{p-2}+1} + \cdots + (a_{n_1} - a_{n_2}) a^{n_1+1} - a_{n_1},$$

we have

$$(a-1)m = A_1 a^{n_p} + A_2,$$

with

$$0 < A_1 < a^{n_r - n_p + 2}, \quad 0 < |A_2| < a^{n_{p-1}+2}.$$

Analogously, defining B_1 and B_2 in a similar way, we have

$$(b-1)m = B_1 b^{\ell_q} + B_2,$$

with

$$0 < B_1 < b^{\ell_t - \ell_q + 2}, \quad 0 < |B_2| < b^{\ell_{q-1}+2}.$$

We observe that

$$1 = \frac{(b-1)(A_1 a^{n_p} + A_2)}{(a-1)(B_1 b^{\ell_q} + B_2)},$$

thus,

$$\begin{aligned} \Lambda := \left| \frac{(b-1)A_1 a^{n_p}}{(a-1)B_1 b^{\ell_q}} - 1 \right| &\le \frac{b-1}{a-1} \left| \frac{A_1 a^{n_p} B_2 - A_2 B_1 b^{\ell_q}}{B_1 b^{\ell_q}(B_1 b^{\ell_q} + B_2)} \right| \\ &\le \frac{|A_2|}{(a-1)m} + \frac{A_1 a^{n_p} B_2}{(a-1)m B_1 b^{\ell_q}} \\ &\ll_{a,b} (a^{-n_r + n_{p-1}} + b^{-\ell_t + \ell_{q-1}}). \end{aligned} \tag{3.31}$$

Assume that $\Lambda = 0$. Then, we have

$$\log \frac{(b-1)A_1}{(a-1)B_1} + n_p \log a - \ell_q \log b = 0. \tag{3.32}$$

By Theorem 2.7, there exist rational integers x_1, x_2, x_3, not all zero, such that

$$x_1 \log \frac{(b-1)A_1}{(a-1)B_1} + x_2 \log a + x_3 \log b = 0 \tag{3.33}$$

and

$$\max\{|x_1|, |x_2|, |x_3|\} \ll_{a,b} \log(A_1 + B_1).$$

Since $s \le k$ and

$$\log A_1 \ll_a \theta^{s-1}, \quad \log B_1 \ll_b \theta^{s-1},$$

we deduce that $|x_2| \ll_{a,b} \theta^{k-1}$ and

$$|x_2| < \frac{\log m}{4 \log a},$$

if m is large enough, by (3.28) and the definition of θ.

Also, using that $n_p \ge n_r - \theta^{s-1}$, we get that

$$n_p > \frac{\log m}{4 \log a},$$

if m is large enough in terms of a and b, thus, $n_p > |x_2|$. Since a and b are multiplicatively independent, x_1 is non-zero. We multiply (3.32) by x_1 and subtract the left-hand side of (3.33) to get

$$(x_1 n_p - x_2) \log a + (x_3 - x_1 \ell_q) \log b = 0.$$

Noticing that $x_1 n_p - x_2$ is non-zero, this contradicts our assumption that a and b are multiplicatively independent.

Consequently, Λ is non-zero. Since $n_p \le n_r \le 2 \log m$ and $\ell_q \le \ell_t \le 2 \log m$, it follows from Theorem 2.2 that

$$\begin{aligned} -\log \left| \frac{(b-1)A_1 a^{n_p}}{(a-1)B_1 b^{\ell_q}} - 1 \right| &\ll_{a,b} \log(A_1 + B_1) \log\log m \\ &\ll_{a,b} (n_r - n_p + \ell_t - \ell_q) \log\log m \\ &\ll_{a,b} \theta^{s-1} \log\log m. \end{aligned} \tag{3.34}$$

On the other hand, we derive from (3.31) that there exist effectively computable positive numbers c_2 and c_3, depending only on a and b, such that

$$-\log \Lambda > c_2 \theta^s - c_3. \tag{3.35}$$

The combination of (3.34) and (3.35) shows that there exists an effectively computable positive real number c_4, depending only on a and b, such that

$$\theta \le c_4 \log\log m.$$

Selecting now $c_1 = 2c_4$, we have reached a contradiction. This shows that (3.29) does not hold, thus, m is bounded from above by an effectively computable number which depends only on a and b. This finishes the proof of the theorem. □

3.10. Further applications (without proofs)

We list below several applications of the theory of linear forms in complex logarithms, which are not related to Diophantine equations. We do not claim to be exhaustive. Our goal is merely to show that this theory applies to a large variety of problems.

– A notorious application of the theory of linear forms in logarithms concerns the Gauss conjecture according to which there are only nine imaginary quadratic fields with class number 1. This was observed by Baker [16] (see also Chapter 5 of [28] and Section 3.1 of [38]), while the conjecture was independently proved by Stark [387] with a different method. Subsequently, Baker [24] and Stark [388] used the theory of linear forms in logarithms of algebraic numbers to prove that all imaginary quadratic fields with class number 2 can be effectively determined; see also [389] and [305,391] for the complete list of these fields. It should be pointed out that this work on class numbers used linear forms whose coefficients are quadratic (and not rational) numbers.

– Chowla raised the question whether there exists a rational valued function $n \mapsto f(n)$, periodic with period a prime number, such that $\sum_{n=1}^{\infty} f(n)/n = 0$. Baker, Birch, and Wirsing [32] used the theory of linear forms in logarithms with algebraic coefficients (an earlier version of Theorem 2.1) to give a negative answer to Chowla question; see also Chapter 23 of [308].

– Let $q \geq 2$ be an integer, χ a non-trivial Dirichlet character modulo q, and set $L(1, \chi) := \sum_{n \geq 1} \frac{\chi(n)}{n}$. Since $L(1, \chi)$ can be expressed as a linear form in $\log(1 - \mathrm{e}^{2\mathrm{i}\pi/q}), \dots$ $\dots, \log(1 - \mathrm{e}^{2\mathrm{i}\pi(q-1)/q})$ with algebraic coefficients, it follows from Theorem 2.1 that $L(1, \chi)$ is transcendental; see Chapters 20 and 25 of [308].

– Adhikari, Saradha, Shorey, and Tijdeman [3] investigated the transcendence of series $S = \sum_{n=0}^{+\infty} f(n)/Q(n)$, where $Q(X)$ is a polynomial with only simple rational roots and $f : \mathbb{Z} \to \overline{\mathbb{Q}}$ is periodic, or $f(X)$ is in $\overline{\mathbb{Q}}[X]$, or f is an exponential polynomial. Roughly speaking, they proved that either S is a computable algebraic number (that is, an algebraic number that can be explicitly determined as a function of its defining parameters), or S is transcendental. The proofs rest mainly on a lower bound for linear forms in logarithms of algebraic numbers with algebraic coefficients, as given in Theorem 2.1.

– Let a, b be multiplicatively independent positive integers. Let ξ be an irrational real number, which is not a Liouville number. By means of Theorem 2.2 (the case $n = 2$), Bourgain, Lindenstrauss, Michel, and Venkatesh [91] proved that the set $\{a^m b^n \xi :$ $0 \leq m, n \leq N\}$, viewed modulo 1, has no gaps of length greater than $(\log \log N)^{-c}$, where the real number c depends on a, b, and the irrationality exponent of ξ. Harrap and Haynes [222] applied Theorem 2.2 to a problem closely related to the Littlewood conjecture in Diophantine approximation.

– Gorodnik and Spatzier [201] used Theorem 2.1 to investigate 3-mixing properties of $\mathbb{Z}^{\ell}$-actions. The parameter B' is crucial in their proof.

– Kühne [247] applied the theory of linear forms in logarithms to give an effective treatment of the André–Oort conjecture for a product of modular curves.

3.11. Exercises

Exercise 3.1. Discuss how Theorem 3.3 extends to multiplicatively independent positive algebraic numbers a and b.

Exercise 3.2 (see [115, 370]). Let $(p_n/q_n)_{n\geq 1}$ be the sequence of convergents to an irrational algebraic number. Establish an effective lower bound for $P[p_n q_n]$.

Exercise 3.3. What can be said if the dominant root is not assumed to be simple in Theorem 3.10? And if y is assumed to be fixed?

Exercise 3.4 (see [122]). Let $f(X)$ be an irreducible integer polynomial of degree at least two and n a positive integer which is not a root of $f(X)$. Establish an effective lower bound for the greatest square free factor of $f(n)$.

Exercise 3.5 (see [294]). Let $\mathbf{u} = (u_n)_{n\geq 0}$ and $\mathbf{v} = (v_m)_{m\geq 0}$ be linear recurrence sequences of integers with a dominant root. Find a condition under which the equation $u_n = v_m$ has only finitely many solutions in integers m, n.

Exercise 3.6 (see [410]). Let $a \geq 2$ be an integer and q an odd prime number. Use Theorem 2.3 to prove that if the integers x, y satisfy $x^2 + a^2 = 2y^q$, then $q \ll \log a$. [Hint. Factor $x^2 + a^2$ over $\mathbb{Z}[\mathrm{i}]$.]

Exercise 3.7 (see [403]). Let a, b, c be integers with $a \geq b > c > 0$. Apply Theorem 2.2 to prove that

$$P[(ab+1)(bc+1)(ca+1)] \gg \log\Big(\frac{\log a}{\log(c+1)}\Big). \tag{3.36}$$

[Hint. Introduce the quantities $\Lambda_1 = \frac{b}{c}\cdot\frac{ac+1}{ab+1} - 1$ and $\Lambda_2 = \frac{(ac+1)(bc+1)}{c^2(ab+1)} - 1$.]

Exercise 3.8 (see [121]). Let $\mathbf{u} := (u_n)_{n\geq 0}$ be a recurrence sequence of integers having a dominant root. Let S be a finite, non-empty set of prime numbers. Prove that there exists an effectively computable positive constant $c(\mathbf{u}, S)$, depending only on $\mathbf{u}$ and S, such that for every positive integer n we have

$$[u_n]_S \ll_{\mathbf{u},S} |u_n|^{1-c(\mathbf{u},S)}.$$

Exercise 3.9. Let $\mathbf{u} := (u_n)_{n\geq 0}$ be a recurrence sequence of integers having a dominant root. Assume that there exist positive integers n, y, q and a non-zero rational number t such that $|u_n| \geq 2$ and $u_n = ty^q$. Prove that we have $q \ll_{\mathbf{u}} \max\{h(t), 1\}$.

3.12. Notes

▷ Kim and Stewart [241] considered the case where the set S in Theorem 3.5 is an infinite set of prime numbers.

▷ Using the hypergeometric method, Bennett, Filaseta, and Trifonov [56, 57] obtained upper bounds for $[n(n+1)]_S$ and $[n^2+7]_S$, where $S = \{2,3\}$ and $S = \{2\}$, respectively. For instance, they established that $[n^2+7]_{\{2\}} < \sqrt{n}$ for every positive integer n not in $\{1, 3, 5, 11, 181\}$ (observe that $1^2+1, 3^2+1, 5^2+1, 11^2+1$, and 181^2+1 are all powers of 2). When applicable, their method gives much stronger numerical results than those obtained by following the proof of Theorem 3.8.

▷ The proof of Theorem 3.9 allows us to get a lower bound for the greatest prime factor of the integer part of $(3/2)^n$; see [277] for related results.

▷ A large variety of results on linear recurrence sequences can be found in the monograph [179]. In many cases, they are established under the dominant root assumption. Sometimes, but not often, this extra assumption can be removed. This is for instance the case for the growth of linear recurrence sequences [180, 337] and for the finiteness of integral values for the ratio of two linear recurrence sequences [156].

▷ Consider the Tribonacci sequence defined by $T_0 = T_1 = 0$, $T_2 = 1$ and the recurrence relation

$$T_{n+3} = T_{n+2} + T_{n+1} + T_n, \quad n \geq 0.$$

Observe that the polynomial $P(X) = X^3 - X^2 - X - 1$ has a real root in the interval $(1, 2)$ and two complex conjugate roots in the open unit disc. Theorem 3.10 applies to show that, for every prime number q large enough, the equation $T_n = y^q$ has no solution with $n \geq 4$. More generally, Pethő [325] established that if $(u_n)_{n \geq 0}$ is a third order recurrence sequence such that its companion polynomial is irreducible and has a dominant root, then there are only finitely many perfect powers in $(u_n)_{n \geq 0}$. This result is, however, not effective and does not enable us to get an upper bound for the largest perfect power in $(u_n)_{n \geq 0}$. As pointed out in [326], we do not even know whether $T_2 = T_3 = 1$, $T_5 = 4$, $T_{10} = 81$, $T_{16} = 3136 = 56^2$, and $T_{18} = 10609 = 103^2$ are the only positive squares in the sequence $(T_n)_{n \geq 0}$.

We can as well define T_n for negative integers n using the same recurrence relation. Then, Theorem 3.10 does not apply anymore to the equation $T_{-n} = y^q$ in positive integers n, y, q, since the companion polynomial $X^3 P(X^{-1})$ has two roots with the same modulus, namely the inverses of the two complex conjugate roots of $P(X)$. This is an open problem [326] to prove that, for every prime number q large enough, the equation $T_{-n} = y^q$ has no solution with $n \geq 4$.

▷ Bugeaud, Cipu, and Mignotte [119] have determined the Fibonacci and Lucas numbers with at most four binary digits. The largest such number is 2584, the eighteenth Fibonacci number, which can be expressed as $2^{11} + 2^9 + 2^4 + 2^3$. For further results on integers having at most three digits in two distinct bases, see [147, 276] and the references quoted therein.

Chapter 4
Classical families of Diophantine equations

In this chapter, we show how the theory of linear forms in logarithms can be applied to prove effective upper bounds for the size of the integer solutions to several classes of Diophantine equations, including unit equations, Thue equations, and superelliptic equations.

We begin by establishing how a weaker version of Theorem 2.2 can be derived from the estimate of linear forms in two logarithms given in Theorem 2.3. Such a weaker version of Theorem 2.2 was obtained by Baker as early as in 1973 (see Theorem 1.10). It is sufficient for proving many results gathered in the present chapter, including Theorems 4.3 to 4.7, but, apparently, not for establishing Theorems 4.9 and 4.11.

4.1. Proof of Baker's Theorem 1.10

Let $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ be complex algebraic numbers. Let $b_1, \dots, b_n$ be non-zero integers and assume that

$$\Lambda := \alpha_1^{b_1} \cdots \alpha_n^{b_n} \alpha_{n+1} - 1 \neq 0.$$

By Liouville's inequality Theorem B.10, there exists a positive real number c, depending only on $\alpha_1, \dots, \alpha_{n+1}$, such that

$$|\Lambda| > \mathrm{e}^{-cB}, \quad \text{where } B := \max\{|b_1|, \dots, |b_n|\}.$$

As mentioned in Chapter 1, Baker established that, if there exists a positive real number δ such that $|\Lambda| < \mathrm{e}^{-\delta B}$, then B is bounded by some quantity depending only on $n, \delta, \alpha_1, \dots, \alpha_n$ times the maximum of 1 and the height of α_{n+1}.

Following an idea of Bombieri and Cohen [86], Bilu and Bugeaud [72] showed how Baker's Theorem 1.10 can be derived from the lower bound for linear forms in two complex logarithms established in [254] and reproduced as Theorem 2.3; see also Theorem 11.1. The next statement was proved in [72]; see also [432].

Theorem 4.1. *Let $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ be complex algebraic numbers in an algebraic number field of degree D. Let $b_1, \dots, b_n$ be non-zero integers and set*

$$B := \max\{|b_1|, \dots, |b_n|\}.$$

If there exists a positive real number δ such that

$$0 < |\alpha_1^{b_1} \cdots \alpha_n^{b_n} \alpha_{n+1} - 1| < \mathrm{e}^{-\delta B}, \tag{4.1}$$

then

$$B \ll_{\alpha_1,\dots,\alpha_n,D,\delta,n} \max\{h(\alpha_{n+1}), 1\}.$$

Clearly, Theorem 4.1 is considerably weaker than Theorem 2.2. However, its proof is much simpler and it is sufficient for many interesting applications, as will be shown in the next sections. A key ingredient is the quantity B' (instead of B) occurring in Theorem 11.1. The proof of Theorem 4.1 actually gives us a more precise upper bound for B, where the dependence of the implied constant is made explicit in terms of $\alpha_1, \dots, \alpha_n, D, \delta, n$. We stress that the present monograph includes a full proof of Theorem 11.1, thus a full proof of Theorem 4.1.

For the proof of Theorem 4.1 we need a special case of a lemma of Bombieri and Cohen [86].

Lemma 4.2. *Let $b_0, b_1, \dots, b_n, N, Q$ be integers with $N \geq Q \geq 2$. There exist a positive integer r and integers $t_0, t_1, \dots, t_n$, not all zero, such that $\lfloor \frac{N}{Q} \rfloor \leq r \leq N$ and*

$$|b_i - rt_i| \leq rQ^{-1/(n+1)} + \frac{|b_i|}{r}, \quad i = 0, \dots, n.$$

Proof. By Minkowski's theorem (see e.g. Chapter II in [357] or Appendix B of [113]) there exist rational integers $t, t_0, t_1, \dots, t_n$, not all zero, such that $|t| \leq Q$ and

$$\left| t\frac{b_i}{N} - t_i \right| \leq Q^{-1/(n+1)}, \quad i = 0, \dots, n. \tag{4.2}$$

We have $t \neq 0$ since, otherwise, we would get $t_0 = t_1 = \cdots = t_n = 0$ by (4.2), which is excluded. Replacing t by $-t$ if necessary, we may assume that $1 \leq t \leq Q$. Let r be the integer part of $\frac{N}{t}$. Since $N \geq Q \geq t \geq 1$, we get $N \geq r \geq \lfloor \frac{N}{Q} \rfloor \geq 1$ and, consequently, for $i = 0, \dots, n$, we have

$$|b_i - rt_i| = \left| r\left(\frac{tb_i}{N} - t_i\right) + \left(\frac{N}{t} - r\right)\frac{b_i t}{N} \right| \leq rQ^{-1/(n+1)} + \frac{|b_i|}{r},$$

as asserted. □

Proof of Theorem 4.1. Keep the assumption of the theorem. Let N and Q be integers which will be chosen later and satisfy

$$B \geq N \geq Q \geq 2. \tag{4.3}$$

Recall that log denotes the principal determination of the logarithm. If $|\alpha_1^{b_1} \cdots \alpha_n^{b_n} \alpha_{n+1} - 1| < \frac{1}{3}$, then there exists an integer b_0, with $|b_0| \leq nB + 1$, such that

$$\Omega := b_0 \log(-1) + b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n + \log \alpha_{n+1}$$

satisfies $|\alpha_1^{b_1} \cdots \alpha_n^{b_n} \alpha_{n+1} - 1| \geq \frac{|\Omega|}{2}$.

Let $r, t_0, t_1, \dots, t_n$ be the integers given by Lemma 4.2 applied to $b_0, b_1, \dots, b_n, N$, and Q. Set $\alpha_0 = -1$, $A_0 := \mathrm{e}^{\pi/D}$,

$$\alpha = \alpha_0^{t_0} \alpha_1^{t_1} \cdots \alpha_n^{t_n}, \quad \text{and} \quad \gamma = \alpha_0^{b_0 - rt_0} \alpha_1^{b_1 - rt_1} \cdots \alpha_n^{b_n - rt_n} \alpha_{n+1}.$$

Define $\ell(\alpha)$ and $\ell(\gamma)$ by

$$\ell(\alpha) = \sum_{i=0}^{n} t_i \log \alpha_i, \quad \ell(\gamma) = \sum_{i=0}^{n} (b_i - rt_i) \log \alpha_i + \log \alpha_{n+1}.$$

We point out that $\ell(\alpha)$ and $\ell(\gamma)$ satisfy $\exp(\ell(\alpha)) = \alpha$ and $\exp(\ell(\gamma)) = \gamma$, respectively, but they have no reason to be the principal determinations of the logarithms of α and γ. We have expressed the linear form Ω as

$$\Omega = r\ell(\alpha) + \ell(\gamma),$$

which is a linear form in two logarithms. We will use Theorem 11.1 to bound $|\Omega|$ from below.

For $i = 0, \dots, n$, observe that

$$|b_i - rt_i| \le rQ^{-1/(n+1)} + \frac{|b_i|}{r} \le rQ^{-1/(n+1)} + \frac{nB+1}{r},$$

$$|t_i| \le \frac{|b_i| + |b_i - rt_i|}{r} \le \frac{nB+1}{r} + \frac{nB+1}{r^2} + Q^{-1/(n+1)} \le \frac{4nB}{r},$$

since $Q^{-1/(n+1)} \le 1 \le \frac{B}{r}$ by (4.3). For $i = 1, \dots, n+1$, define A_i by

$$\log A_i := \max\left\{h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D}\right\}.$$

We deduce the estimates

$$\max\left\{h(\alpha), \frac{|\ell(\alpha)|}{D}, \frac{1}{D}\right\} \le \sum_{i=0}^{n} |t_i| \log A_i \le \frac{4nB}{r} \sum_{i=0}^{n} \log A_i, \tag{4.4}$$

$$\begin{aligned}\max\left\{h(\gamma), \frac{|\ell(\gamma)|}{D}, \frac{1}{D}\right\} &\le \sum_{i=0}^{n} |b_i - rt_i| \log A_i + \log A_{n+1} \\ &\le \left(rQ^{-1/(n+1)} + \frac{2nB}{r}\right) \sum_{i=0}^{n} \log A_i + \log A_{n+1}.\end{aligned} \tag{4.5}$$

Assume that Q satisfies the inequality

$$B \ge \max\left\{4Q^{2+1/(n+1)}, 2(\log A_{n+1})Q^{1+1/(n+1)}\right\} \tag{4.6}$$

and set

$$N = Q\left\lceil \max\left\{B^{1/2}Q^{1/(2n+2)}, (\log A_{n+1})Q^{1/(n+1)}\right\}\right\rceil.$$

Then, (4.3) holds and we get the upper bounds (4.4) and (4.5). Furthermore, $r \ge \lfloor \frac{N}{Q} \rfloor = \frac{N}{Q}$ implies $\frac{B}{r} \le rQ^{-1/(n+1)}$ and $\log A_{n+1} \le rQ^{-1/(n+1)}$. The former inequality, combined with (4.5), gives

$$\max\left\{h(\gamma), \frac{|\ell(\gamma)|}{D}, \frac{1}{D}\right\} \le 3nrQ^{-1/(n+1)}\,(1 + \log A_0 + \log A_1 + \cdots + \log A_n) =: G.$$

Since Ω is non-zero, it follows from Theorem 11.1 that

$$\log|\Omega| \gg -D^4 \frac{nB}{r}\Big(\sum_{i=0}^{n} \log A_i\Big) G\Big(\log\Big(\frac{r}{G}+2\Big)\Big)^2$$

and there exists an effectively computable positive real number c_1 such that

$$\log\frac{|\Omega|}{2} > -c_1 n^2 B D^4 Q^{-1/(n+1)}\Big(\sum_{i=0}^{n} \log A_i\Big)^2 (\log Q)^2.$$

Setting

$$\delta := c_1 n^2 D^4 Q^{-1/(n+1)}\Big(\sum_{i=0}^{n} \log A_i\Big)^2 (\log Q)^2, \tag{4.7}$$

we have established that

$$\log|\alpha_1^{b_1}\cdots\alpha_n^{b_n}\alpha_{n+1} - 1| \geq -\delta B.$$

This contradicts our assumption (4.1), thus (4.6) does not hold and we get

$$B < \max\big\{4Q^{2+1/(n+1)}, 2(\log A_{n+1})Q^{1+1/(n+1)}\big\} \tag{4.8}$$

Setting $\widetilde{\delta} := \min\{\delta, 1\}$, we deduce from (4.7) that

$$Q \leq (c_2 n)^{4n} D^{4(n+1)} \widetilde{\delta}^{-n-1}\Big(\sum_{i=0}^{n} \log A_i\Big)^{2(n+1)} \Big(\log\Big(nD\widetilde{\delta}^{-1}\Big(\sum_{i=0}^{n} \log A_i\Big)\Big)\Big)^{2(n+1)},$$

where c_2 is an effectively computable positive real number. The theorem then follows from (4.8) and the fact that

$$\log A_{n+1} = \max\Big\{h(\alpha_{n+1}), \frac{|\log\alpha_{n+1}|}{D}, \frac{1}{D}\Big\} \leq h(\alpha_{n+1}) + \frac{\pi}{D},$$

by the definition of the height. □

4.2. The unit equation

Let K be an algebraic number field. Many Diophantine problems reduce to equations of the form

$$\alpha x + \beta y = 1,$$

where α, β are given elements of K and the unknowns x, y are elements of its unit group O_K^*. These equations are called *unit equations*. Explicit upper bound for the solutions of unit equations were given for the first time by Győry [210]; see also Bugeaud and Győry [124], Győry and Yu [217], and the monographs [182, 183] by Evertse and Győry, where the reader can find many bibliographic references and numerous applications.

Theorem 4.3. *Let K be an algebraic number field of degree d and discriminant D_K. Let α, β be non-zero elements of K. The unit equation*

$$\alpha x + \beta y = 1 \tag{4.9}$$

has only finitely many solutions in algebraic units x and y in O_K^*, and all of them satisfy

$$\max\{h(x), h(y)\} \ll_{d,D_K} \max\{h(\alpha), h(\beta), 1\}. \tag{4.10}$$

Proof. Let x, y be in O_K^* such that (4.9) holds. We assume that $h(x) \geq h(y)$. Let r be the unit rank of K and $\{\eta_1, \dots, \eta_r\}$ a fundamental system of units in K satisfying the inequalities stated in Lemma C.4. Then, we can write

$$y = \zeta \eta_1^{b_1} \dots \eta_r^{b_r}, \tag{4.11}$$

where ζ is a root of unity in K and $b_1, \dots, b_r$ are rational integers.

Put $B := \max\{|b_1|, \dots, |b_r|, 3\}$ and let $v_1, \dots, v_{r+1}$ denote the non-equivalent complex places on K. Then (4.11) implies that

$$\log |y|_{v_j} = \sum_{i=1}^{r} b_i \log |\eta_i|_{v_j}, \quad j = 1, \dots, r.$$

Using Cramer's rule and the definition of the height, we deduce from (4.11) and Lemma C.4 that

$$B \ll_{d,D_K} h(y) \ll_{d,D_K} B. \tag{4.12}$$

Let v be a complex place for which $|x|_v$ is minimal. It then follows from Definition B.4 that

$$h(x) = h\left(\frac{1}{x}\right) \leq -\log |x|_v.$$

Assume, without any loss of generality, that $h(x) \geq 2dh(\alpha)$. Then, we deduce from (4.12) that

$$\begin{aligned} \log |\alpha x|_v \leq \log |\alpha|_v + \log |x|_v \leq dh(\alpha) - h(x) &\leq -\frac{h(x)}{2} \\ &\leq -\frac{h(y)}{2} \ll_{d,D_K} (-B). \end{aligned} \tag{4.13}$$

Let σ be a complex embedding such that $|x|_v = |\sigma(x)|$. By setting $\alpha_{r+1} = \zeta\beta$ we deduce from (4.9) that

$$|\alpha x|_v = |\eta_1^{b_1} \dots \eta_r^{b_r} \alpha_{r+1} - 1|_v = |\sigma(\eta_1)^{b_1} \dots \sigma(\eta_r)^{b_r} \sigma(\alpha_{r+1}) - 1|. \tag{4.14}$$

It then follows from (4.13) and Theorem 4.1 that

$$B \ll_{d,D_K} \max\{h(\alpha_{r+1}), 1\} \ll_{d,D_K} \max\{h(\beta), 1\},$$

thus, by (4.11),

$$h(y) \ll_{d,D_K} B \ll_{d,D_K} \max\{h(\beta), 1\}.$$

We deduce from Theorem B.5 that

$$\begin{aligned} h(x) &\le h(\alpha x) + h(\alpha) + \log 2 \\ &\le h(y) + h(\beta) + h(\alpha) + \log 4 \ll_{d,D_K} \max\{h(\alpha), h(\beta), 1\}. \end{aligned}$$

By Northcott's Theorem B.7, this implies that (4.9) has only finitely many solutions in x, y in O_K^* and completes the proof of the theorem. □

If we are interested in the size of the constant implicit in $\ll_{d,D_K}$, a better result follows by applying Theorem 2.2 directly to (4.14) rather than using Theorem 4.1; see Section 6.6.

Observe that the upper bound in (4.10) is linear in $\max\{h(\alpha), h(\beta), 1\}$. This is ultimately a consequence of the quantity B' occurring in the estimates of linear forms in logarithms.

4.3. The Thue equation

Let $F(X, Y)$ be an homogeneous, binary, integer polynomial of degree at least three and such that $F(X, 1)$ has at least three distinct roots. Let m be a non-zero integer. In 1909, Axel Thue [412] established that the equation

$$F(x, y) = m, \quad \text{in integers } x, y,$$

has only finitely many solutions. This equation is called the Thue equation. Thue's method, however, does not yield upper bounds for the absolute values of its solutions. The first general effective result on Thue's equations was established by Baker [20]. We also refer to [33, 125, 216] and the monograph [182] for general totally explicit statements, and to [125, 182, 216, 376] for an extensive list of bibliographic references and applications.

Theorem 4.4. *Let $F(X, Y)$ be an homogeneous, irreducible polynomial with integer coefficients and of degree at least three. Let m be a non-zero integer. Then, there exists a positive real number C, depending only on $F(X, Y)$, such that all the integer solutions x, y to the Diophantine equation*

$$F(x, y) = m$$

satisfy $\max\{|x|, |y|\} \le |2m|^C$.

We establish a more general statement, which will be needed in Section 4.5.

Theorem 4.5. *Let K be an algebraic number field of degree d and discriminant D_K. Let $n \ge 3$ be an integer and $\alpha_1, \dots, \alpha_n$ distinct algebraic numbers in K. Let a and m be non-zero algebraic integers in K. Then, the equation*

$$a(x - \alpha_1 y) \cdots (x - \alpha_n y) = m \tag{4.15}$$

has only finitely many solutions in algebraic integers x and y in K, and all of them satisfy

$$\max\{h(x), h(y)\} \ll_{n,d,D_K,a,\underline{\alpha}} \max\{h(m), 1\}, \tag{4.16}$$

where $\underline{\alpha}$ denotes the n-tuple $(\alpha_1, \dots, \alpha_n)$.

The assumption $n \geq 3$ cannot be replaced by $n \geq 2$ in view of the Pellian equation.

Theorem 4.5 not only shows that the heights of x and y are effectively bounded, but also that the bound is linear in $\max\{h(m), 1\}$. Again, this is ultimately a consequence of the introduction of the quantity B' in the estimates for linear forms in logarithms.

Proof. Let x and y be algebraic integers in K satisfying (4.15). Multiplying both sides of (4.15) by a^{n-1} times a suitable positive integer depending on $\alpha_1, \dots, \alpha_n$, we see that we may assume in the sequel that $a = 1$ and that $\alpha_1, \dots, \alpha_n$ are algebraic integers. Suppose also that the heights of x and y are very large in terms of d, D_K, and $\underline{\alpha}$. By applying if needed a complex embedding of K, we may assume that

$$\log \max\{|x|, |y|\} \gg_d \max\{h(x), h(y), 1\}. \tag{4.17}$$

There exists at most one index i such that

$$|x - \alpha_i y| < \frac{|y|}{2} \cdot \min_{1 \leq j < k \leq n} |\alpha_j - \alpha_k|.$$

Since the heights of x and y are supposed to be sufficiently large, it follows from (4.15) and (4.17) that this index exists and, without any loss of generality, we take $i = 1$. We then get $|x| \ll_{\underline{\alpha}} |y|$ and, successively, the inequalities

$$\begin{aligned} &|x - \alpha_j y| \gg_{\underline{\alpha}} \max\{|x|, |y|\}, \quad j = 2, \dots, n, \\ &|x - \alpha_1 y| \ll_{n,\underline{\alpha}} |m| \max\{|x|, |y|\}^{-n+1}. \end{aligned} \tag{4.18}$$

We also assume that $\max\{|x|, |y|\} \geq |m|$ (otherwise, (4.16) clearly holds) and get

$$|x - \alpha_1 y| \ll_{n,\underline{\alpha}} \max\{|x|, |y|\}^{-n+2}. \tag{4.19}$$

Set

$$\beta_j = x - \alpha_j y, \quad j = 1, 2, 3,$$

and observe that

$$(\alpha_1 - \alpha_2)\beta_3 + (\alpha_2 - \alpha_3)\beta_1 + (\alpha_3 - \alpha_1)\beta_2 = 0.$$

Consider the quantity

$$\Lambda := \frac{\alpha_2 - \alpha_3}{\alpha_3 - \alpha_1} \cdot \frac{x - \alpha_1 y}{x - \alpha_2 y} = \frac{x - \alpha_3 y}{x - \alpha_2 y} \cdot \frac{\alpha_2 - \alpha_1}{\alpha_3 - \alpha_1} - 1\ .$$

Let r be the rank of the group of units of the field $L := K(\alpha_1, \alpha_2, \alpha_3)$ and $\eta_1, \dots, \eta_r$ a system of fundamental units of L satisfying the inequalities stated in Lemma C.4. Note that the degree of L is at most equal to d^3 and the absolute value of its discriminant is bounded from above in terms of $\alpha_1, \alpha_2, \alpha_3, d$, and D_K, by Lemma C.7.

By Proposition C.5, there exist algebraic integers γ_2, γ_3 in L and integers $b_1, \dots, b_r$, $c_1, \dots, c_r$ such that

$$x - \alpha_2 y = \gamma_2 \eta_1^{b_1} \dots \eta_r^{b_r}, \quad x - \alpha_3 y = \gamma_3 \eta_1^{c_1} \dots \eta_r^{c_r},$$
$$h(\gamma_2), h(\gamma_3) \ll_{d, D_K, \underline{\alpha}} \log |2 \operatorname{Norm}_{L/\mathbb{Q}} m|, \tag{4.20}$$

and

$$\begin{aligned} B &:= \max\{|b_1|, \dots, |b_r|, |c_1|, \dots, |c_r|\} \\ &\ll_{d, D_K, \underline{\alpha}} \big(1 + h(x - \alpha_2 y) + h(x - \alpha_3 y)\big) \ll_{d, D_K, \underline{\alpha}} X, \end{aligned} \tag{4.21}$$

where $X := \max\{h(x), h(y), 1\}$. It follows from (4.17), (4.18), (4.19), and (4.21) that

$$\log |\Lambda| \ll_{n,d,D_K,\underline{\alpha}} (-\log \max\{|x|, |y|\}) \ll_{n,d,D_K,\underline{\alpha}} (-X) \ll_{n,d,D_K,\underline{\alpha}} (-B). \tag{4.22}$$

Observe that

$$\Lambda = \eta_1^{c_1 - b_1} \dots \eta_r^{c_r - b_r} \frac{\gamma_3(\alpha_2 - \alpha_1)}{\gamma_2(\alpha_3 - \alpha_1)} - 1.$$

Write $\nu := \gamma_3(\alpha_2 - \alpha_1)/(\gamma_2(\alpha_3 - \alpha_1))$ and note that $h(\nu) \ll_{d, D_K, \underline{\alpha}} \log M$, where we have set $M := |2 \operatorname{Norm}_{L/\mathbb{Q}} m|$. We immediately deduce from (4.22) and Theorem 4.1 that

$$B \ll_{n,d,D_K,\underline{\alpha}} \max\{h(\nu), 1\} \ll_{n,d,D_K,\underline{\alpha}} \log M. \tag{4.23}$$

Using (4.20) to bound the heights of

$$(\alpha_3 - \alpha_2)x = \alpha_3(x - \alpha_2 y) - \alpha_2(x - \alpha_3 y)$$

and $(\alpha_3 - \alpha_2)y$, we get

$$h(x), h(y) \ll_{d, D_K, \underline{\alpha}} (B + \log M). \tag{4.24}$$

Thus, by (4.23), we obtain

$$X \ll_{n,d,D_K,\underline{\alpha}} \log M.$$

Since $\log M \ll_d \max\{h(m), 1\}$, this proves (4.16) and we deduce from Northcott's Theorem B.7 that (4.15) has only finitely many solutions x, y in K. This completes the proof of the theorem.

Instead of using Theorem 4.1, we can as well apply Theorem 2.2, which gives

$$\log |\Lambda| \gg_{n,d,D_K,\underline{\alpha}} -h(\nu) \log\Big(1 + \frac{B}{h(\nu)}\Big),$$

so that, by (4.21), we obtain

$$\frac{B}{h(\nu)} \ll_{n,d,D_K,\underline{\alpha}} \log\left(1 + \frac{B}{h(\nu)}\right).$$

From this, we deduce that

$$B \ll_{n,d,D_K,\underline{\alpha}} \max\{h(\nu), 1\} \ll_{n,d,D_K,\underline{\alpha}} \log M,$$

and we conclude by using (4.24). This more direct proof yields the best known explicit bounds. □

4.4. Effective improvement of Liouville's inequality

An outstanding open problem in Diophantine approximation is to establish an effective version of Roth's Theorem A.7. Results in this direction were given in Section 3.4 for specific classes of algebraic numbers. In 1968 Feldman [185] was the first to prove that the effective irrationality exponent of an arbitrary real algebraic number of degree greater than two is strictly less than its degree.

The present textbook contains a full proof of Theorem 4.6, which is derived from an estimate for linear forms in only two complex logarithms; see [72].

Theorem 4.6. *Let α be an algebraic number of degree $n \geq 3$. Then, there exists an effectively computable positive real number $\tau(\alpha)$, depending only on α, such that*

$$\mu_{\mathrm{eff}}(\alpha) \leq n - \tau(\alpha).$$

Proof. Set $\alpha_1 = \alpha$ and let $a(X-\alpha_1)\cdots(X-\alpha_n)$ with $a \geq 1$ denote the minimal defining polynomial of α over the integers. Let x and y be non-zero integers and set $X := \max\{|x|, |y|\}$. It follows from Theorem 4.4 that there exists an effectively computable positive number C, depending only on α, such that

$$|x - \alpha y| \geq \frac{X^{1/C}}{2a|x-\alpha_2 y| \ldots |x - \alpha_n y|} \gg_\alpha X^{-(n-1)+1/C}.$$

This proves the theorem. □

It follows from Theorem A.4 that Theorem 4.6 cannot hold for quadratic numbers; see, however, Theorem 6.3 for a result of a similar flavour valid for quadratic numbers.

4.5. The superelliptic and hyperelliptic equations

In 1926 Siegel [377] established that, for any integers m, n with $m \geq 3$ and $n \geq 2$, for any non-zero integers a, b, and k, the equation

$$ax^m - by^n = k, \quad \text{in integers } x, y,$$

has only finitely many solutions. His method does not enable us to compute upper bounds for $|x|$ and $|y|$. However, this can be achieved since the end of the '60s, as one of the many applications of the theory of linear forms in logarithms; see [21, 22] and [92, 101] for more recent and more general results.

Theorem 4.7. *Let $f(X)$ be an integer polynomial of degree m without multiple roots, and let n be an integer. Assume that $m \geq 2$, $n \geq 2$, and $mn \geq 6$. Let t be a non-zero integer. Then, every solution in integers x, y to*

$$f(x) = ty^n \tag{4.25}$$

satisfies $\max\{|x|, |y|\} \ll_{f,t,n} 1$.

Proof. Let K be the splitting field of $f(X)$. By multiplying both sides of (4.25) by the $(m-1)$-th power of the leading coefficient of $f(X)$, we can assume that $f(X)$ is monic.

Assume first that $n \geq 3$. It follows from Proposition C.6 and Theorem B.5 that there exist distinct roots α_1, α_2 of $f(X)$, algebraic integers γ_1, γ_2 in K, and β_1, β_2 in K such that

$$x - \alpha_1 = \beta_1 \gamma_1^n, \quad x - \alpha_2 = \beta_2 \gamma_2^n,$$

and

$$h(\beta_1), h(\beta_2) \ll_{n,t,f} 1.$$

By Northcott's Theorem B.7, this shows that the pair (β_1, β_2) belong to a finite set of pairs of algebraic numbers and that (γ_1, γ_2) is solution to the Thue equation (over the number field K)

$$\beta_1 X^n - \beta_2 Y^n = \alpha_2 - \alpha_1. \tag{4.26}$$

Since the polynomial $\beta_1 X^n - \beta_2$ has $n \geq 3$ distinct roots, it follows from Theorem 4.5 that (4.26) has only finitely many solutions in algebraic integers X, Y in K, thus the set of quadruples $(\beta_1, \beta_2, \gamma_1, \gamma_2)$ is finite. Furthermore, we get an effective upper bound for the heights of γ_1 and γ_2, hence for $|x|$ and $|y|$, in terms of $f(X)$, t, and n.

The case $n = 2$ is slightly more involved. It follows from Proposition C.6 and Theorem B.5 that there exist distinct roots $\alpha_1, \alpha_2, \alpha_3$ of $f(X)$, algebraic integers $\gamma_1, \gamma_2, \gamma_3$ in K, and $\beta_1, \beta_2, \beta_3$ in K such that

$$x - \alpha_1 = \beta_1 \gamma_1^2, \quad x - \alpha_2 = \beta_2 \gamma_2^2, \quad x - \alpha_3 = \beta_3 \gamma_3^2.$$

and

$$h(\beta_1), h(\beta_2), h(\beta_3) \ll_{t,f} 1.$$

By Northcott's Theorem B.7, this shows that the triple $(\beta_1, \beta_2, \beta_3)$ belongs to a finite set of triples of algebraic numbers. For $i = 1, 2, 3$, fix a square root $\beta_i^{1/2}$ of β_i. Set $L = K(\beta_1^{1/2}, \beta_2^{1/2}, \beta_3^{1/2})$. Since

$$\alpha_i - \alpha_j = \beta_j \gamma_j^2 - \beta_i \gamma_i^2, \quad \text{for } 1 \leq i < j \leq 3,$$

the norms over $\mathbb{Q}$ of $\beta_j^{1/2} \gamma_j - \beta_i^{1/2} \gamma_i$, where $1 \leq i < j \leq 3$, are bounded in terms of $f(X)$ only. Put

$$\delta_1^- = \beta_2^{1/2} \gamma_2 - \beta_3^{1/2} \gamma_3, \quad \delta_2^- = \beta_3^{1/2} \gamma_3 - \beta_1^{1/2} \gamma_1, \quad \delta_3^- = \beta_1^{1/2} \gamma_1 - \beta_2^{1/2} \gamma_2,$$
$$\delta_1^+ = \beta_2^{1/2} \gamma_2 + \beta_3^{1/2} \gamma_3, \quad \delta_2^+ = \beta_3^{1/2} \gamma_3 + \beta_1^{1/2} \gamma_1, \quad \delta_3^+ = \beta_1^{1/2} \gamma_1 + \beta_2^{1/2} \gamma_2.$$

For $i = 1, 2, 3$, we can write

$$\delta_i^- = \nu_i^- \varepsilon_i^-, \quad \delta_i^+ = \nu_i^+ \varepsilon_i^+,$$

where, by Proposition C.5, ν_i^-, ν_i^+ are in L and have their heights bounded in terms of $f(X)$ and the degree and discriminant of L, and $\varepsilon_i^-, \varepsilon_i^+$ are unknown units in L.

We check that

$$\nu_1^+\varepsilon_1^+ - \nu_2^+\varepsilon_2^+ + \nu_3^-\varepsilon_3^- = 0$$

and

$$\nu_1^+\varepsilon_1^+ - \nu_2^-\varepsilon_2^- - \nu_3^+\varepsilon_3^+ = 0.$$

It then follows from Theorem 4.3 on unit equations that $h(\varepsilon_1^+/\varepsilon_3^-)$ and $h(\varepsilon_1^+/\varepsilon_3^+)$ are bounded in terms of $f(X)$ and the degree and discriminant of L. Since

$$\alpha_2 - \alpha_1 = \delta_3^-\delta_3^+ = \nu_3^-\nu_3^+\varepsilon_3^-\varepsilon_3^+,$$

we get

$$(\varepsilon_1^+)^2 = \frac{\varepsilon_1^+}{\varepsilon_3^+} \cdot \frac{\varepsilon_1^+}{\varepsilon_3^-} \cdot \frac{\alpha_2 - \alpha_1}{\nu_3^-\nu_3^+}.$$

This implies that the height of ε_1^+ and, consequently, the height of δ_1^+ are bounded in terms of $f(X)$ and the degree and discriminant of L. The same conclusion holds for the heights of ε_1^- and δ_1^-. Since

$$(\delta_1^- + \delta_1^+)^2 = 4\beta_2\gamma_2^2 = 4(x - \alpha_2),$$

it then follows that $|x|$ is bounded in terms of $f(X)$ and the degree and discriminant of L. Note that the degree of L is at most equal to 8 times the degree of K. Furthermore, by Lemma C.7, the discriminant of L is effectively bounded in terms of the discriminant of K, the degree of L, and the heights of $\beta_1, \beta_2, \beta_3$, which are all $\ll_{t,f} 1$. Since K is the splitting field of $f(X)$, its discriminant and height are $\ll_f 1$. Putting all this together, we have established that $\max\{|x|, |y|\} \ll_{f,t} 1$. This completes the proof of the theorem. □

4.6. The Diophantine equation $x^2 + C = y^n$

The Diophantine equation $x^2 + 1 = y^n$ was solved in 1850 by V. A. Lebesgue [256] by means of an elegant 2-adic argument; see Section 2.1 of [73]. Since then, many mathematicians have investigated the equation

$$x^2 + C = y^n, \tag{4.27}$$

where C is a fixed non-zero integer and x, y, n are unknown integers with $n \geq 3$. We do not consider the case $n = 2$, since it reduces to $(x + y)(x - y) = -C$, which is easy to solve. For references on the case C positive, the reader is directed to [138, 155] and the articles quoted therein.

A major difference between the cases C negative and C positive is the existence of values of C for which $x^2 + C = y^n$ has a solution for every (odd) value of n. This happens precisely when C is negative and equal to minus a square plus or minus one. In that case, the equation $x^2 + C = \pm 1$ has a solution and this prevents the direct use of congruences to solve completely $x^2 + C = y^n$ for $n \geq 3$ odd, since $y = 1$ or $y = -1$ gives then always a solution. Obviously, this situation cannot occur for positive values of C.

Ramanujan [343] noticed that the equation $x^2 + 7 = 2^n$ has at least 5 solutions in positive integers x, n, given by $x = 1, 3, 5, 11$, and 181. Subsequently, Nagell [310, 311] (see also his collected papers [313]) established in 1948 that there are no more solutions and, nowadays, this equation is called the Ramanujan–Nagell equation. This is the most famous special case of (4.27).

All the solutions of (4.27) with $1 \leq C \leq 100$ are listed at the end of [138]. The hundred corresponding equations are not all equally difficult to solve. Below we focus our attention on three specific values of C, namely $2, 7$, and 25, and explain how one derives a linear form in logarithms from each of the corresponding equations. For a further discussion on the equation $x^2 + C = y^n$, see the short Section 7.3. Section 7.4 is devoted to the number of solutions to the equation $x^2 + D = p^n$.

Theorem 4.8. *The only solutions in positive integers x, y, n to the generalised Ramanujan–Nagell equation*

$$x^2 + 7 = y^n, \quad n \geq 3,$$

satisfy $x = 1, 3, 5, 11, 181$. *The only solutions in positive integers x, y, n to the equations $x^2 + 2 = y^n$ and $x^2 + 25 = y^n$ with $n \geq 3$ satisfy $x = 5$ and $x = 10$, respectively.*

Outline of the proof. In the sequel, we assume that $x \geq 20$ and n is an odd prime number q.

Let x, y, q be such that $x^2 + 2 = y^q$. Arguing modulo 4, we see that, since $q \geq 3$, the integer x must be odd. Write

$$x^2 + 2 = (x + \mathrm{i}\sqrt{2})(x - \mathrm{i}\sqrt{2}).$$

Since every common divisor of $x + \mathrm{i}\sqrt{2}$ and $x - \mathrm{i}\sqrt{2}$ also divides their difference $2\mathrm{i}\sqrt{2}$, we deduce from the fact that x is odd that $x + \mathrm{i}\sqrt{2}$ and $x - \mathrm{i}\sqrt{2}$ are coprime. The ring $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ is a unique factorization domain, thus there exist rational integers a, b such that

$$x + \mathrm{i}\sqrt{2} = (a + \mathrm{i}b\sqrt{2})^q. \tag{4.28}$$

The quantity

$$\Lambda_2 := \Big| \Big(\frac{a + \mathrm{i}b\sqrt{2}}{a - \mathrm{i}b\sqrt{2}} \Big)^q - 1 \Big| = \Big| \frac{x + \mathrm{i}\sqrt{2}}{x - \mathrm{i}\sqrt{2}} - 1 \Big|$$

is very small, bounded from above by $\frac{4}{x}$. Since the Galois conjugate of $\zeta := a + \mathrm{i}b\sqrt{2}$ is equal to its inverse and

$$\zeta + \zeta^{-1} = \frac{2(a^2 - 2b^2)}{a^2 + 2b^2},$$

we get

$$h(\zeta) \ll \log(a^2 + b^2) \ll \frac{\log x}{q}.$$

It then follows from Theorem 2.6 that

$$\log 4 - \log x \geq \log \Lambda_2 \gg -\frac{\log x}{q} (\log q)^2,$$

and we derive an absolute upper bound on q. This bound, obtained by means of an estimate of linear forms in two logarithms, is rather small. Then, for each value of q between 5 and this bound, sieving by several prime numbers congruent to 1 modulo q, we can rather quickly establish that $x^2 + 2 = y^q$ has no solutions. If $x^2 + 2 = y^3$, then we get

$$x + \mathrm{i}\sqrt{2} = a(a^2 - 6b^2) + \mathrm{i}b(3a^2 - 2b^2)\sqrt{2},$$

thus $b = 1$ and $a = \pm 1$. This shows that $5^2 + 2 = 3^3$ is the only solution of $x^2 + 2 = y^3$ in positive integers.

Instead of Theorem 2.6, we could of course use Theorem 2.2 and get $q \ll \log q$, but the numerical upper bound for q will then be larger, because of the larger size of the numerical constant in Theorem 2.2.

Let x, y, q be such that $x^2 + 7 = y^q$. We work in the ring $\mathbb{Z}[(1 + \mathrm{i}\sqrt{7})/2]$, which is a unique factorization domain. Write $x^2 + 7 = (x + \mathrm{i}\sqrt{7})(x - \mathrm{i}\sqrt{7})$. Every common divisor of $x + \mathrm{i}\sqrt{7}$ and $x - \mathrm{i}\sqrt{7}$ also divides their difference $2\mathrm{i}\sqrt{7}$. Since

$$2 = \Big(\frac{1 + \mathrm{i}\sqrt{7}}{2}\Big) \cdot \Big(\frac{1 - \mathrm{i}\sqrt{7}}{2}\Big),$$

we deduce that there exist rational integers a, b, and ε in $\{\pm 1\}$ such that

$$x + \mathrm{i}\sqrt{7} = \Big(\frac{1 + \varepsilon\mathrm{i}\sqrt{7}}{2}\Big)\,(a + \mathrm{i}b\sqrt{7})^q. \tag{4.29}$$

Again, the quantity

$$\Lambda_7 := \Big|\Big(\frac{1 + \varepsilon\mathrm{i}\sqrt{7}}{1 - \varepsilon\mathrm{i}\sqrt{7}}\Big)\Big(\frac{a + \mathrm{i}b\sqrt{7}}{a - \mathrm{i}b\sqrt{7}}\Big)^q - 1\Big| = \Big|\frac{x + \mathrm{i}\sqrt{7}}{x - \mathrm{i}\sqrt{7}} - 1\Big|$$

is very small, bounded from above by $\frac{9}{x}$. As above, we check that

$$h\Big(\frac{a + \mathrm{i}b\sqrt{7}}{a - \mathrm{i}b\sqrt{7}}\Big) \ll \log(a^2 + b^2) \ll \frac{\log x}{q}.$$

As already mentioned before the statement of Theorem 2.2, the fact that Λ_7 is smaller than $\frac{9}{x}$ does not imply that the linear form

$$\Big|\log\Big(\frac{1 + \varepsilon\mathrm{i}\sqrt{7}}{1 - \varepsilon\mathrm{i}\sqrt{7}}\Big) + q\log\Big(\frac{a + \mathrm{i}b\sqrt{7}}{a - \mathrm{i}b\sqrt{7}}\Big)\Big|$$

is smaller than $\frac{18}{x}$. It only implies the existence of an integer b_0 with $|b_0| \le 1 + q$ such that

$$\Big|b_0\log(-1) + \log\Big(\frac{1 + \varepsilon\mathrm{i}\sqrt{7}}{1 - \varepsilon\mathrm{i}\sqrt{7}}\Big) + q\log\Big(\frac{a + \mathrm{i}b\sqrt{7}}{a - \mathrm{i}b\sqrt{7}}\Big)\Big| \le \frac{18}{x}.$$

We then deduce from Theorem 2.2 that

$$\log 18 - \log x \ge \log\Lambda_7 \gg -\frac{\log x}{q}\,(\log q).$$

Again, we get an absolute upper bound on q, but it is much bigger than in the case of the equation $x^2 + 2 = y^q$, since we were forced to use a lower bound for three (instead of two) logarithms. A careful reader may observe that an upper bound for q can also be deduced from Theorem 4.1, thus, ultimately follows from Theorem 2.3. However, if we proceed along these lines, then we end up with a much larger upper bound than the one obtained by applying Theorem 2.2 in the way explained above.

Let x, y, q be such that $x^2 + 25 = y^q$. Observe that $x^2 + 25 = (x + 5\mathrm{i})(x - 5\mathrm{i})$. Arguing modulo 2 we deduce that x must be even. If 5 does not divide x, then the greatest common divisor of $x + 5\mathrm{i}$ and $x - 5\mathrm{i}$ divides 2, thus, since x is even, $x + 5\mathrm{i}$ and $x - 5\mathrm{i}$ are coprime. Consequently, there exist rational integers a, b such that

$$x + 5\mathrm{i} = (a + \mathrm{i}b)^q.$$

We then proceed as in the case of the equation $x^2 + 2 = y^q$ and derive an upper bound for q from an estimate of a linear form in two logarithms. We omit the details.

The difficulty occurs when 5 divides x. Indeed, 5 must then divide y as well, and we end up with the Diophantine equation

$$x^2 + 1 = 5^{q-2} y^q. \tag{4.30}$$

Noticing that $5 = (2 + \mathrm{i})(2 - \mathrm{i})$, we factor (4.30) in the ring of Gaussian integers and eventually derive a linear form in three logarithms. This allows us to compute an upper bound for q. Again, we leave the details to the reader.

For an arbitrary value of C, a further difficulty occurs in the resolution of $x^2 + C = y^q$ when the class number of the quadratic field generated by $\sqrt{C}$ is divisible by the prime number q, because such a factoring as in (4.28) or (4.29) is not possible anymore. In this case, the standard method consists in reducing $x^2 + C = y^q$ to Thue equations of degree q; see e.g. [138, 301]. □

4.7. Perfect powers at integer values of polynomials

As already observed in Section 3.7, the theory of linear form in complex logarithms also allows us to bound effectively the size of the solutions to Diophantine equations, even when exponents are unknown. The next result was proved by Schinzel and Tijdeman [356] and, subsequently, generalized by Shorey [369], with a simpler proof; see also [61, 95, 100]. A proof of Theorem 4.9 in the special case where $f(X)$ has at least two simple rational zeros was given in a survey paper of Tijdeman [417]. While ineffective versions of Theorems 4.5 and 4.7 were established before the theory of linear forms in logarithms, no proof of Theorem 4.9 based on the ideas of Thue and Siegel is known.

Theorem 4.9. *Let $f(X)$ be an integer polynomial of degree $n \geq 2$ without multiple roots. Set $z_0 = 3$ if $n = 2$ and $z_0 = 2$ otherwise. Let t be a non-zero integer. Then, every integer solution (x, y, z) with $z \geq z_0$ and $|y| \geq 2$ to*

$$f(x) = ty^z \tag{4.31}$$

satisfies $\max\{|x|, |y|, z\} \ll_{t,f} 1$.

Proof. We follow an argument of Brindza, Evertse, and Győry [95]. Multiplying both sides of (4.31) by the $(n-1)$-th power of the leading coefficient of $f(X)$, we can assume that $f(X)$ is monic. Our goal is to bound z in terms of $f(X)$ and t since, in view of Theorem 4.7, this is sufficient to conclude.

Let H be the maximum of the absolute values of the coefficients of $f(X)$. Let $\alpha_1, \dots, \alpha_n$ denote its roots and observe that they are bounded in modulus by $H+1$.

Let (x, y, z) be a solution of (4.31). If $|x| \le 2(H+1)$, then we have

$$2^z \le |ty^z| = |x-\alpha_1| \cdots |x-\alpha_n| \le (3H+3)^n.$$

We can therefore assume that $|x| > 2(H+1)$, which implies that $|x-\alpha_j| \ge \frac{|x|}{2} > 1$ and $|x-\alpha_j| \le |ty^z|$ for $j = 1, \dots, n$. We can as well assume that $|x| > |y|^{z/(2n)}$. Indeed, otherwise, we would get $|x-\alpha_j| \le 2|x| \le 2|y|^{z/(2n)}$ for $j = 1, \dots, n$, thus

$$|y^z| \le |f(x)| \le 2^n |y|^{z/2},$$

giving $z \log |y| \le 2n \log 2$ and $z \le 2n$.

Assume first that $f(X)$ has an irrational root α_1. Let $f_1(X)$ be the minimal defining polynomial of α_1. Set $K = \mathbb{Q}(\alpha_1)$ and let h_K denote its class number. By Proposition C.6, there exist algebraic integers $\beta_1, \gamma_1, \delta_1$ in K and a unit ζ_1 in K such that

$$\delta_1 \, (x-\alpha_1)^{h_K} = \zeta_1 \, \beta_1 \, \gamma_1^z \tag{4.32}$$

and

$$\max\{h(\delta_1), h(\beta_1)\} \ll_{t,f} 1. \tag{4.33}$$

Let α_2 denote a root of $f_1(X)$, distinct from α_1, and denote by σ the complex embedding sending α_1 to α_2. For simplicity, for any τ in $\mathbb{Q}(\alpha_1)$, we write τ^σ instead of $\sigma(\tau)$. Then, by applying σ to (4.32), we get

$$\delta_1^\sigma \, (x-\alpha_2)^{h_K} = \zeta_1^\sigma \, \beta_1^\sigma \, (\gamma_1^\sigma)^z. \tag{4.34}$$

We may assume that

$$4h_K(H+1) < 2^{z/(4n)}, \tag{4.35}$$

since otherwise the theorem is proved. From $|x-\alpha_1| \ge \frac{|x|}{2}$ and $|x| > |y|^{z/(2n)}$, we get

$$\left| \frac{\alpha_1 - \alpha_2}{x - \alpha_1} \right| \le \frac{4(H+1)}{|y|^{z/(2n)}}.$$

Without any loss of generality, we may assume that $|x-\alpha_2| \le |x-\alpha_1|$. Then, by (4.35), we obtain the upper estimate

$$\Lambda := \left| \left(\frac{x-\alpha_2}{x-\alpha_1} \right)^{h_K} - 1 \right| \le \left| \frac{x-\alpha_2}{x-\alpha_1} - 1 \right| \cdot h_K \le \frac{4h_K(H+1)}{|y|^{z/(2n)}} < \frac{1}{|y|^{z/(4n)}}. \tag{4.36}$$

Let $\{\eta_1, \dots, \eta_r\}$ be a fundamental system of units in $\mathbb{Q}(\alpha_1)$. By (4.32) and (4.34), there exist ξ_1 in K and integers $k_1, \dots, k_r$ of absolute values less than z such that

$$\left(\frac{x-\alpha_2}{x-\alpha_1} \right)^{h_K} = \frac{\beta_1^\sigma}{\beta_1} \frac{\delta_1}{\delta_1^\sigma} \left(\frac{\eta_1^\sigma}{\eta_1} \right)^{k_1} \cdots \left(\frac{\eta_r^\sigma}{\eta_r} \right)^{k_r} \left(\frac{\xi_1^\sigma}{\xi_1} \right)^z. \tag{4.37}$$

Furthermore, the height of $x-\alpha_1$ being $\ll_t z \log |y|$, we get

$$h(\xi_1) \ll_{t,f} \log |y|. \tag{4.38}$$

If $\Lambda = 0$, then $(\alpha_1-\alpha_2)/(x-\alpha_1)$ is an algebraic integer and we derive that $|x| \ll_f 1$. It then follows from (4.31) that $z \ll_f 1$.

If $\Lambda \neq 0$, then we deduce from Theorem 2.2, (4.33), (4.37), and (4.38) that

$$\log \Lambda \gg_{t,f} \bigl(-\max\{1, h(\xi_1)\}(\log z)\bigr) \gg_{t,f} (-\log |y| \cdot \log z). \tag{4.39}$$

Comparing (4.36) and (4.39), we obtain

$$z \ll_{t,f} \log z.$$

This proves that z is bounded in terms of t and $f(X)$. It then only remains to apply Theorem 4.7 to conclude the proof of the theorem when $f(X)$ has an irrational root.

When $f(X)$ has only rational roots, the proof follows the same lines, but is much simpler. Since $f(X)$ is monic, its roots are integers. Then, there exist rational numbers d_1, d_2 and integers y_1, y_2 such that

$$x-\alpha_1 = d_1 y_1^z, \quad x-\alpha_2 = d_2 y_2^z,$$

where numerators and denominators of d_1 and d_2 are $\ll_{t,f} 1$. The quantity $|(x-\alpha_1)/(x-\alpha_2)|$ is close to 1 when $|x|$ is large, and we directly apply Theorem 2.2 to bound z from above. We leave the details to the reader. □

4.8. The Catalan equation and the Pillai conjecture

In a letter written in 1844 to August Leopold Crelle, Eugène Catalan [145] addressed the following question: do there exist consecutive positive integers other than 8 and 9 which are both perfect powers? Said differently, is $3^2 - 2^3 = 1$ the only solution to the exponential Diophantine equation

$$x^m - y^n = 1, \tag{4.40}$$

in the four integer unknowns x, y, m, n all greater than 1? This problem has been solved completely in 2002 by Mihăilescu [71, 302].

THEOREM 4.10. *The integers* 8 *and* 9 *are the only consecutive positive integers which are both perfect powers.*

Even if Mihăilescu managed to remove any use of estimates for linear forms in logarithms in his latest proof of Theorem 4.10, it remains of interest to study how the theory of linear forms in logarithms can be applied to show that (4.40) has only finitely many solutions, a result which was established in 1976 by Tijdeman [416]. The reader interested in a complete proof of Mihăilescu's theorem may consult [73, 152, 154, 362].

THEOREM 4.11. *If x, y, m, n are integers at least equal to* 2 *such that $x^m - y^n = 1$, then* $\max\{x, y, m, n\} \ll 1$.

Proof. By Theorem 4.7 the equations $y^2 + 1 = x^m$ and $x^2 - 1 = y^n$ have only finitely many solutions, which can be effectively bounded. Thus, we may assume that m and n are odd. It is sufficient to consider the equation

$$x^m - y^n = \varepsilon,$$

where $\varepsilon = \pm 1$ and x, y, m, n are positive integers with $n > m > 2$.

Since, for every integer $c \geq 2$, every odd integer $\ell \geq 3$, and η in $\{-1, 1\}$ we have

$$\frac{c^\ell + \eta}{c + \eta} = \ell + (c + \eta) \sum_{1 \leq k \leq \ell - 1} (-1)^{\ell - k - 1} \binom{\ell}{k + 1} (c + \eta)^{k-1},$$

it follows that the greatest common divisor of $\frac{c^\ell + \eta}{c + \eta}$ and $c + \eta$ divides ℓ. Thus, there exist positive integers m^*, n^*, u, v, with $u \geq 2$ and $v \geq 2$, such that

$$x - \varepsilon = \frac{u^n}{m^*}, \quad y + \varepsilon = \frac{v^m}{n^*},$$

and m^* (*resp.,* n^*) is a divisor of m (*resp.,* of n). In particular, we get that

$$x + 1 \geq \frac{u^n}{m} > \frac{u^n}{n},$$

thus

$$\log x \gg n \log u \gg m. \tag{4.41}$$

It follows from the assumption $n > m$ that $x > y$. By (4.41), we get

$$\Lambda_1 := \left| \left(\frac{y}{u^m} \right)^n (m^*)^m - 1 \right| = \left| \frac{y^n}{u^{mn} (m^*)^{-m}} - 1 \right| = \left| \frac{x^m - \varepsilon}{(x - \varepsilon)^m} - 1 \right| \ll \frac{m}{x},$$

thus

$$\log \Lambda_1 \ll -\log x.$$

Since

$$y^n \leq x^m + 1 \leq (u^n + 1)^m + 1 \leq 2^m u^{nm},$$

we get the upper bound $y \leq 2u^m$. By Theorem 2.2, we then obtain

$$\log \Lambda_1 \gg -(m \log u) (\log m) (\log n),$$

thus,

$$\log x \ll m (\log m) (\log n) (\log u).$$

By the first inequality of (4.41), this gives

$$n \ll m (\log m) (\log n). \tag{4.42}$$

We deduce from (4.42) that

$$y + 1 \geq \frac{v^m}{n} \gg \frac{v^m}{m^2} \gg v^{m/2},$$

thus, again by (4.42),

$$\log y \gg m \log v \gg \sqrt{n} \log v. \tag{4.43}$$

Consequently,

$$\Lambda_2 := \left|\left(\frac{u}{v}\right)^{mn} (m^*)^{-m} (n^*)^n - 1\right| = \left|\frac{u^{mn}}{(m^*)^m} \frac{(n^*)^n}{v^{mn}} - 1\right| = \left|\frac{(x-\varepsilon)^m}{(y+\varepsilon)^n} - 1\right| \ll \frac{n}{y}$$

and

$$\log \Lambda_2 \ll -\log y.$$

Then, we deduce from $u \le 3v$ (whose proof is left to the reader) and Theorem 2.2 that

$$\log \Lambda_2 \gg -(\log v)\,(\log m)\,(\log n)\,(\log mn),$$

thus,

$$\log y \ll (\log mn)\,(\log m)\,(\log n)\,(\log v).$$

Hence, by the first inequality of (4.43), we obtain

$$m \ll (\log m)\,(\log n)^2. \tag{4.44}$$

Combining inequalities (4.42) and (4.44) we find that n and m are bounded by an absolute real number. The fact that x and y are also bounded from above follows from general results on superelliptic Diophantine equations given in Theorem 4.7. □

Shortly after the publication of Tijdeman's proof, Langevin [251] computed explicit (albeit huge) upper bounds for the solutions of the Catalan equation (4.40); he showed that

$$y^n, x^m < \exp\exp\exp\exp 730.$$

The proof of Theorem 4.11 involves estimates for linear forms in two logarithms and in three logarithms. Since, regarding the numerical constant, the current state-of-the-art for linear forms in three logarithms is not as good as in the case of two logarithms, we cannot hope to get very small upper bounds for the exponents in (4.40). Nevertheless, Mignotte [297] established that, if p and q are odd prime numbers such that $x^p - y^q = 1$ has a solution in positive integers x, y, then

$$\min\{p, q\} < 7.15 \times 10^{11}.$$

There are various criteria to ensure that, for a given pair of odd prime numbers (p, q), the equation $x^p - y^q = 1$ has no solution in positive integers x, y. By means of these criteria, Mignotte [297] proved that $\min\{p, q\} > 10^7$. This lower bound was improved to 3.2×10^8 by extensive computations made by Grantham and Wheeler (see [46]). However, there remains a gap and it is not clear whether an alternative proof of Theorem 4.10 can be obtained along these lines.

The Pillai conjecture is a natural generalization of Catalan's problem.

Conjecture 4.12 (Pillai's conjecture). *Let a, b, and k be non-zero integers. Then, the Diophantine equation*

$$ax^m - by^n = k, \quad \text{in integers } m, n, x, y \text{ with } m \geq 3,\ n \geq 2,\ x \geq 2, \text{ and } y \geq 2, \tag{4.45}$$

has only finitely many solutions.

In 1936, at the end of [331], the Indian mathematician Pillai formulated the special case $a = b = 1$ of the above conjecture (see also his paper [332]), which is, however, commonly referred to as "Pillai's conjecture". Also, equation (4.45) is usually called the Pillai equation. We emphasize that there is no triple of relatively prime integers a, b, k with $|abk| \geq 2$ for which the corresponding equation (4.45) is known to have only finitely many solutions. In particular, we still do not know whether the difference between two consecutive perfect powers tends to infinity.

As a consequence of Theorems 3.10 and 4.9, we get the following theorem, whose proof is left as an exercise.

Theorem 4.13. *The Pillai equation (4.45) has only finitely many solutions when one among the four variables x, y, m, n is fixed.*

4.9. Exercises

Exercise 4.1. Follow the proof of Theorem 4.9 to establish that, if $f(X)$ is an integer polynomial of degree at least two (*resp.*, three) and without multiple roots and if t is a non-zero rational number, then every integer solution (x, y, z) with $z \geq 3$ (*resp.*, $z \geq 2$) to (4.31) satisfies $z \ll_f \max\{h(t), 1\}$. [This result is apparently new; it slightly improves Theorem 2.1 on page 145 of [386].]

Exercise 4.2. Prove Theorem 4.13.

4.10. Notes

▷ Baker and Stewart [36] established effective irrationality measures for cubic real numbers.

▷ Bombieri [84] (see also [86, 87] and his survey [85]) gave an alternative proof of Theorem 4.6, independent of the theory of linear forms in logarithms; see [107] for a combination of both methods.

▷ For specific algebraic numbers α, it is sometimes possible to derive a much better effective irrationality exponent than the one given in Theorem 4.6. The first result of this type (although a forerunner is implicit in early works of Thue [412, 413]) was obtained in 1964 by Alan Baker [15], who established that 2.955 is an effective irrationality exponent of $\sqrt[3]{2}$. More recent works include [43, 82, 83, 89, 90, 148, 165].

▷ Solving unit equations, Thue equations, and superelliptic equations is essentially equivalent; see [261]. The theory of linear forms in logarithms has been used by Baker and Coates [33] and, subsequently, by Schmidt [358] to give effectively computable upper bounds for the height of integer points on curves of genus one. Effective results for linear equations in two unknowns from a multiplicative division group have been given in [60]; see also [182]. Effective upper bounds for the size of solutions to further families of Diophantine equations can be found in the monographs [182, 183, 376, 386] and in the papers [68–70].

▷ Let K be a number field. Shafarevich's theorem asserts that, for a given finite set of places S of K, there are only finitely many elliptic curves E defined over K with good reduction outside of S. An effective version of this theorem, whose proof rests on the theory of linear forms in logarithms, has been given by Fuchs, von Känel, and Wüstholz [188]. It has been extended to hyperelliptic curves by von Känel [235]; see also the monograph [183].

▷ Two monic integer polynomials $f(X), g(X)$ are called equivalent if $g(X) = f(X+a)$ for some integer a. Equivalent polynomials have the same discriminant. Using effective results on unit equations, Győry [209] proved that for any given non-zero integer D, there are only finitely many inequivalent monic polynomials with discriminant D and they can be effectively determined. For quantitative versions, generalisations, and various applications, see e.g. [183, 210].

▷ The only reference on the equation $x^2 - C = y^n$, where C is a fixed positive integer, seems to be the unpublished PhD thesis of Carlos Barros [41].

▷ For the algorithmic resolution of Diophantine equations, the reader is directed to the monographs [153, 154, 191, 382] and Chapter 5 of [182]. Efficient algorithms to solve Thue equations of high degree and superelliptic equations are given and discussed in [74–76]. The complete resolution of equations of the form $f(x) = y^n$ with n fixed remains rather difficult when n is not very small; see, however, [127].

▷ Starting with a seminal paper of Emery Thomas [411], there is an extensive literature on parametric families of Thue equations; see for example the survey of Heuberger [227]. Hoshi [233] managed to solve completely a parametric family of Thue equations of degree 12.

▷ Pethő [322] used an explicit estimate of Sprindžuk [386] for the integer solutions of equations of the form $f(x) = ty^2$ to establish that, for every quadratic number α and every integer $q \geq 2$, we have $\|q^2\alpha\| \gg_\alpha (\log q)^{0.0005} q^{-2}$.

▷ An explicit lower bound for the difference between two perfect powers is given in [429]. For more information on the Pillai equation, the reader is referred to the survey [435]. Theorem 4.11 has been extended to number fields by Brindza, Győry, and Tijdeman [97].

▷ Let $F(X, Y)$ be an irreducible, homogeneous polynomial of degree three with integer coefficients. Bennett and Dahmen [55] established that the generalized superelliptic equation $F(x, y) = z^\ell$, in integers x, y, z, ℓ with $\gcd(x, y) = 1$, $|z| \geq 2$, and $\ell \geq 4$, has finitely many solutions. They also obtained analogous results for polynomials of degree 4, 6, and 12. Their proof does not use estimates for linear forms in logarithms. It proceeds via construction of Frey curves corresponding to putative solutions to $F(x, y) = z^\ell$ and rests on the so-called modular method, based upon modularity of Galois representations.

Chapter 5
Further applications

We have pointed out in Chapter 2 that estimates for linear forms in logarithms are considerably better when the algebraic numbers involved are very close to 1. This chapter is devoted to some spectacular applications of this theoretical refinement.

5.1. Effective irrationality measures for quotients of logarithms of rational numbers

Theorem 3.3 asserts that the quotient of the logarithms of two positive, multiplicatively independent rational numbers $\frac{a_1}{a_2}, \frac{b_1}{b_2}$ is not a Liouville number and, more precisely, that its irrationality exponent is bounded from above by some absolute real number times the product of $\log \max\{a_1, a_2\}$ and $\log \max\{b_1, b_2\}$. The next result shows that we get an absolute upper bound for this irrationality exponent when $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ are very close to 1. Its proof and a slightly more general statement are given in [116]; see Exercise 5.1.

Theorem 5.1. *Let a_1, a_2, b_1, b_2 be integers such that*

$$36 \le a_2 < a_1 < a_2 + \sqrt{a_1}, \quad 36 \le b_2 < b_1 < b_2 + \sqrt{b_1}, \quad \text{and} \quad \sqrt{b_1} < a_1 < b_1^2.$$

If $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ are multiplicatively independent, then we have

$$\mu_{\text{eff}}\left(\frac{\log \frac{a_1}{a_2}}{\log \frac{b_1}{b_2}}\right) \le 221105. \tag{5.1}$$

Proof. We show only that the irrationality exponent in (5.1) is bounded from above by an absolute, effectively computable real number. Let $\frac{x}{y}$ be a convergent to $(\log \frac{a_1}{a_2})/(\log \frac{b_1}{b_2})$ with $y \ge 3$. Set $X := \max\{|x|, |y|\}$. We need to estimate from below the quantity

$$\left|\frac{\log \frac{a_1}{a_2}}{\log \frac{b_1}{b_2}} - \frac{x}{y}\right| = \frac{1}{y}\left|y \log \frac{a_1}{a_2} - x \log \frac{b_1}{b_2}\right|.$$

We apply Theorem 2.1 with the parameter E given by

$$E := \min\{\sqrt{a_1}, \sqrt{b_1}\}.$$

Observe that

$$\log\Big(\frac{a_1}{a_2}\Big) = \log\Big(1 + \frac{a_1 - a_2}{a_2}\Big) \le \frac{a_1 - a_2}{a_2} \le \frac{\sqrt{a_1}}{a_2},$$

thus

$$\frac{\log a_1}{\log \frac{a_1}{a_2}} \ge \frac{a_2(\log a_1)}{\sqrt{a_1}} \ge \sqrt{a_1} \ge \mathrm{e} \quad \text{and} \quad \log a_1 \ge E \log \frac{a_1}{a_2}.$$

Likewise, we check that

$$\frac{\log b_1}{\log \frac{b_1}{b_2}} \ge \sqrt{b_1} \ge \mathrm{e} \quad \text{and} \quad \log b_1 \ge E \log \frac{b_1}{b_2}.$$

It then follows from Theorem 2.1 applied with $A_1 = a_1, A_2 = b_1$, and $E^* = E$ that

$$\log \Big| y \log \frac{a_1}{a_2} - x \log \frac{b_1}{b_2} \Big| \gg -(\log a_1)(\log b_1)(\log X)(\log E)^{-2}. \tag{5.2}$$

Consequently, we have proved that

$$\mu_{\text{eff}}\left(\frac{\log \frac{a_1}{a_2}}{\log \frac{b_1}{b_2}} \right) \ll \frac{(\log a_1)(\log b_1)}{(\log E)^2} \ll \frac{(\log a_1)(\log b_1)}{\min\{\log a_1, \log b_1\}^2} \ll 1.$$

This completes the proof of Theorem 5.1, up to the value of the numerical constant. □

It is crucial in the proof of Theorem 5.1 that the dependence on X occurs in (5.2) through the factor $\log X$, and not $(\log X)^2$, which would have been given by Theorem 2.4. Actually, in [116], we have applied an estimate of Gouillon [202], which improves the numerical constants of Theorem 2.1 in the case of two logarithms. This explains the (relatively) small size of the numerical value in (5.1).

5.2. Effective irrationality measures for n-th roots of rational numbers

By Theorem 3.6, for positive integers a, b, n with $n \ge 3$ and $a > b$, the effective irrationality exponent of $\sqrt[n]{a/b}$ satisfies

$$\mu_{\text{eff}}(\sqrt[n]{a/b}) \ll (\log a)(\log n), \tag{5.3}$$

which improves Liouville's bound when n is large enough. If, moreover, a exceeds 2^n, then the factor $(\log n)$ in (5.3) can be removed.

It was observed in [117] that, as an immediate consequence of Theorem 2.5, the upper bound (5.3) can be dramatically improved when the rational number $\frac{a}{b}$ is very close to 1.

Theorem 5.2. *Let a, b, n be integers with $n \ge 3$ and $1 < b < a \le \frac{6b}{5}$. Define η in $(0, 1]$ by $a - b = ba^{-\eta}$. Then, we have*

$$\mu_{\text{eff}}(\sqrt[n]{a/b}) \le \frac{35.2}{\eta} \max\Big\{1 + \frac{\log n}{\eta \log a}, 10\Big\}^2.$$

Consequently, if $b < a < b\bigl(1 + \frac{1}{\sqrt{a}}\bigr)$ *and* $a \geq n^{2/9}$*, then we get*

$$\mu_{\mathrm{eff}}(\sqrt[n]{a/b}\,) \leq 7040.$$

Proof. We proceed as in the proof of Theorem 3.6. Let a, b, n, η be as above and $\frac{p}{q}$ a convergent to $\sqrt[n]{a/b}$ with $q \geq 100$. Since $\frac{a}{b} = 1 + a^{-\eta}$, it follows from Theorem 2.5 that

$$\log\Bigl|\Bigl(\frac{q}{p}\Bigr)^n \frac{a}{b} - 1\Bigr| \geq -\frac{35.2}{\eta}\,(\log p)\,\Bigl(\max\Bigl\{1 + \frac{\log n}{\eta \log a}, 10\Bigr\}\Bigr)^2.$$

This gives the first assertion of the theorem. The second one follows by choosing $\eta = \frac{1}{2}$. □

Theorem 5.2 should be compared with a result of Bombieri and Mueller [89], who established that, if a, b, n are positive integers with $b \geq 2$ and $n \geq 3$ such that $\sqrt[n]{a/b}$ is of degree n, then, defining η' by

$$|a - b| = b^{1-\eta'}$$

and assuming that $n > 2/\eta'$, we get

$$\mu_{\mathrm{eff}}(\sqrt[n]{a/b}\,) \leq \frac{2}{\eta'} + 6\sqrt[3]{\frac{n^5 \log n}{\log b}}. \tag{5.4}$$

It follows from (5.4) that, for any positive real number ε and any integer $n \geq 3$, we have $\mu_{\mathrm{eff}}(\sqrt[n]{a/b}) < 2 + \varepsilon$ if b is sufficiently large in terms of n and if $\frac{a}{b}$ is sufficiently close to 1. Such a remarkable result does not follow from Theorem 5.2. However, we stress that (5.4) improves Liouville's bound only when b is very large compared to n; namely, one requires that b satisfies

$$b > n^{216n^2},$$

while the much weaker assumption $b > n^{2/9}$ is sufficient to apply Theorem 5.2.

5.3. The Thue equation $ax^n - by^n = c$

In this section we consider the binary Thue equation

$$ax^n - by^n = c, \tag{5.5}$$

where a, b, c, and n are non-zero fixed integers, with a, b positive, $n \geq 3$, and where x and y are unknown integers. We show that it has no non-trivial solutions x, y (that is, no solutions with $|xy| \geq 2$) when a and b are close to each other, $|c|$ is small, and n is large enough. We start with a more general result.

Theorem 5.3. *Let a, b, and c be non-zero integers with* $a > b \geq 1$ *and* $|c| \leq b$*. If*

$$n \geq \max\Bigl\{2 \log \frac{|c|}{a - b}, 15000 \log a\Bigr\},$$

then the Thue equation

$$ax^n - by^n = c \tag{5.6}$$

has no integer solutions x, y with $|xy| \geq 2$.

Proof. Let x, y be integers with $|xy| \geq 2$ and satisfying (5.6). If $|x| \geq |y|$, then

$$|c| = |ax^n - by^n| \geq (a-b)|x|^n \geq (a-b)2^n,$$

giving $n < 2\log(|c|/(a-b))$.

Thus, we assume that $|y| > |x|$. Dividing both sides of (5.6) by by^n, we get

$$\left|\frac{a}{b}\left(\frac{x}{y}\right)^n - 1\right| \leq \frac{|c|}{b|y|^n} \leq \frac{1}{|y|^n}.$$

Theorem 2.3 implies that

$$-n\log|y| \geq -25.4\,(\log\max\{\mathrm{e}, a\})\log|y|\ \max\left\{\log\left(\frac{n}{\log\max\{\mathrm{e}, a\}}\right) + 0.21, 20\right\}^2,$$

which gives

$$n < 15000\log a.$$

This completes the proof of the theorem. □

We see from the proof of Theorem 5.3 that if a is very close to b, then the rational numbers $\frac{a}{b}$ and $\frac{x}{y}$ are both very close to 1. We may thus expect to get a stronger result in this particular case. This is indeed what happens, as was first proved by Mignotte [296]. We display a special case of a result from [296].

Theorem 5.4. *If there exist positive integers n, b, c, x, y with $n \geq 3$, $\max\{x, y\} > 1$, $c \geq 5$, and $b \geq c^2$, satisfying*

$$|(b+c)x^n - by^n| \leq c,$$

then $n < 7500$.

We point out that the upper bound for n in Theorem 5.4 is independent of b and c.

Proof. We follow the proof of Theorem 5.3, but instead of applying Theorem 2.3, we use Theorem 2.5. Write

$$\Lambda := \frac{b+c}{b}\left(\frac{x}{y}\right)^n - 1$$

and observe that $y > x$ and

$$\log|\Lambda| \leq -n\log y. \tag{5.7}$$

Apply Theorem 2.5 with $x_2 = b + c$ and $y_2 = b$. Let η_0 be defined by

$$\eta_0 = \frac{\log\frac{b}{c}}{\log(b+c)}$$

and note that

$$\eta_0 \geq \frac{\log b}{2\log(b+c)} \geq \frac{\log 25}{2\log 30} \geq 0.47.$$

Then, we get

$$\log|\Lambda| \geq -\frac{35.2}{0.47}(\log y)\big(\max\{1+\log n, 10\}\big)^2.$$

Combined with (5.7), this gives

$$n < 7500.$$

This proves the theorem. □

Equation (5.5) with $c = 1$ has been considered by Bennett and de Weger [59] and, subsequently, by Bennett [45], who established the following definitive result.

Theorem 5.5. *Let a, b, n be positive integers with $n \geq 3$. Then, the equation*

$$|ax^n - by^n| = 1$$

has at most one solution in positive integers x and y.

Theorem 5.5 gives us the complete list of solutions to the two-parametric family of Thue equations $(b+1)x^n - by^n = \pm 1$.

5.4. A generalization of Diophantine quadruples

In the present section, we study a variant of the problem of Diophantus discussed in Section 3.8, namely the existence of triples $\{a, b, c\}$ of positive integers such that the three numbers $ab + 1$, $ac + 1$ and $bc + 1$ are perfect k-th powers, for a fixed integer $k \geq 3$. Examples of such triples for $k = 3$ and $k = 4$ are given, respectively, by $\{2, 171, 25326\}$ and $\{1352, 9539880, 9768370\}$. To our knowledge, no example of such a triple is known for an integer $k \geq 5$. The next theorem was established in [120].

Theorem 5.6. *Let $k \geq 3$ and $0 < a < b < c < d$ be integers such that the four numbers*

$$ac + 1, \quad ad + 1, \quad bc + 1, \quad \textit{and} \quad bd + 1$$

are perfect k-th powers. Then we have $k \leq 176$. Consequently, for any integer $k \geq 177$, there exist no set of four positive integers such that the product of any two of them increased by 1 is a perfect k-th power.

Proof. We content ourselves to prove that k is bounded by 80000. Let a, b, c, d be integers with $0 < a < b < c < d$ such that there exist positive integers r, s, t, u, and $k \geq 2$ with

$$ac + 1 = r^k, \quad ad + 1 = s^k, \quad bc + 1 = t^k, \quad \text{and} \quad bd + 1 = u^k.$$

Set

$$\alpha_1 = \frac{ur}{st}, \quad \alpha_2 = \frac{b}{a} \cdot \frac{ac+1}{bc+1}.$$

Observe that $\alpha_1 > 1$ since the product $(b-a)(d-c)$ is positive. Furthermore, α_2 and $\alpha_1^{-k}\alpha_2$ are very close to 1, namely,

$$|\alpha_2 - 1| = \alpha_2 - 1 = \frac{b-a}{abc+a} < \frac{1}{c} \tag{5.8}$$

and

$$\Lambda := \left| \left(\frac{st}{ur} \right)^k \left(\frac{b}{a} \cdot \frac{ac+1}{bc+1} \right) - 1 \right| = \frac{b(ad+1)}{a(bd+1)} - 1 = \frac{b-a}{a(bd+1)} < \frac{1}{d}. \tag{5.9}$$

We apply Theorem 2.5 with $\frac{x_1}{y_1} = \alpha_1$ and $\frac{x_2}{y_2} = \alpha_2$ in order to bound Λ from below. By (5.8), the parameter η satisfies

$$\eta := \frac{-\log(\alpha_2 - 1)}{\log b(ac+1)} > \frac{\log c}{\log b(ac+1)}.$$

It then follows from Theorem 2.5 that

$$\log \Lambda \geq -35.2 \frac{\log b(ac+1)}{\log c} (\log ur) \big(\max\{1 + \log k, 10\}\big)^2. \tag{5.10}$$

Using that $b(ac+1) \leq c^3$, we derive from (5.9) and (5.10) that

$$k \log d \leq 105.6\, k (\log ur) \big(\max\{1 + \log k, 10\}\big)^2.$$

Since

$$k(\log ur) \leq \log(2abcd) \leq 5 \log d,$$

we obtain

$$k \leq 528 \big(\max\{1 + \log k, 10\}\big)^2,$$

giving an absolute upper bound for k, namely $k \leq 80000$. □

5.5. Exercises

Exercise 5.1 (see [116]). Let ε be a real number with $0 < \varepsilon < 1$. Let a_1, a_2, b_1, b_2 be integers such that

$$2 \leq a_2 < a_1 < a_2 + a_1^{1-\varepsilon}, \quad 2 \leq b_2 < b_1 < b_2 + b_1^{1-\varepsilon}, \quad \text{and} \quad b_1^{\varepsilon} < a_1 < b_1^{1/\varepsilon}.$$

Prove that

$$\mu_{\mathrm{eff}} \left(\frac{\log \frac{a_1}{a_2}}{\log \frac{b_1}{b_2}} \right) \ll \varepsilon^{-4}.$$

Exercise 5.2 (see [47, 112]). Prove that all the solutions to the Diophantine equation $(x^k - 1)(y^k - 1) = (z^k - 1)$, in positive integers x, y, z, k with $z \geq 2$, satisfy $k \ll 1$.

Exercise 5.3 (see [114]). Let η be a positive real number. Let α, β be real algebraic integers such that $\alpha + \beta$, $\alpha\beta$ are rational integers and $\alpha \geq |\beta|^{1+\eta}$. Prove that all the solutions in positive integers n, q, y of

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = y^q,$$

with q prime, n congruent to 1 modulo q, and $|y| \geq 2$, satisfy $q \ll \eta^{-3}$.

5.6. Notes

▷ The first applications of Shorey's idea [367, 368] appeared in [366]. Subsequently, Ramachandra, Shorey, and Tijdeman [341, 342] applied linear forms in logarithms of algebraic numbers close to 1 to investigate Grimm's conjecture on factorisation of blocks of consecutive integers (see Problem 13.21).

▷ Further applications of estimates for linear forms in logarithms of algebraic numbers close to 1 can be found in the survey [114].

▷ In various Diophantine problems, linear forms in logarithms of algebraic numbers close to 1 are used to give an explicit upper bound for an unknown exponent. When this exponent is assumed to be fixed, it is often possible to use the hypergeometric method to show the finiteness of the number of solutions to the corresponding equation. This was done e.g. in [120], where the authors established, for any integer k with $11 \leq k \leq 176$, the finiteness of the set of quadruples $\{a, b, c, d\}$ of positive integers such that the product of any two of them increased by 1 is a k-th power. Other papers combining estimates for linear forms in logarithms of algebraic numbers close to 1 and the hypergeometric method include [112, 136, 140, 231, 350].

▷ Theorem 5.6 suggests to consider sets $\{a_1, \dots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a perfect power for all i, j with $1 \leq i < j \leq m$; see [123, 207, 208, 275, 397]. Estimates for linear forms in four logarithms were used by Luca in [275]. The main result of [208] was obtained by a modification of Luca's argument allowing the authors to apply linear forms in only two logarithms. Finally, Stewart [397] managed to use estimates for simultaneous linear forms in logarithms (see Chapter 9) to prove that the cardinality of a subset A of $\{1, 2, \dots, n\}$ such that $ab + 1$ is a perfect power for every distinct a, b in A cannot exceed some absolute constant times $(\log n)^{2/3}(\log\log n)^{1/3}$.

Chapter 6
Applications of linear forms in p-adic logarithms

In the present chapter, we emphasize several applications of estimates for linear forms in p-adic logarithms, often in combination with estimates for linear forms in complex logarithms. Among other results, we extend the effective estimates for the size of the solutions of classical families of Diophantine equations obtained in Chapter 4: we give effective upper bounds not only for the integer solutions, but also for the solutions in rational numbers, whose denominators are composed of prime numbers from a given, finite set.

6.1. On the p-adic distance between two integral S-units

The following result can be viewed as a p-adic analogue to Theorem 3.4. It shows that two distinct integral S-units cannot be p-adically too close.

Theorem 6.1. *Let S denote a finite, non-empty set of prime numbers and $(x_j)_{j\ge 1}$ the increasing sequence of all positive integers whose prime factors belong to S. Let p be a prime number not in S. There exists a real number c, which can be explicitly computed in terms of the prime numbers in S, such that*

$$|x_j - x_h|_p \ge (\log x_j)^{-cp/(\log p)}, \quad 1 \le h < j. \tag{6.1}$$

We point out that the dependence on p in Theorem 6.1 is rather weak. It is very likely that the exponent of $(\log x_j)$ in (6.1) should be independent of p. However, this exponent cannot be smaller than 1. To see this, let J be a large integer and set $\ell := \lceil (\log J)/(\log p) \rceil - 1$. By the Dirichlet *Schubfachprinzip*, there exist integers h, k such that $1 \le h < k \le J$ and x_h and x_k are in the same congruence class modulo p^ℓ. Since $(x_j)_{j\ge 1}$ grows at most exponentially fast, there exists a real number κ, which can be explicitly computed in terms of the prime numbers in S, such that

$$|x_h - x_k|_p \le p^{-\ell} \le pJ^{-1} \le \kappa p\,(\log x_J)^{-1}.$$

Proof of Theorem 6.1. Write $S = \{q_1, \dots, q_s\}$, where $q_1, \dots, q_s$ are prime numbers with $q_1 < \cdots < q_s$. Let u, v with $2 \le u < v$ be two elements of the sequence $(x_j)_{j\ge 1}$ and write

$$u = \prod_{i=1}^{s} q_i^{u_i}, \quad v = \prod_{i=1}^{s} q_i^{v_i}.$$

Without any loss of generality, we can assume that u and v are coprime, thus, for $i = 1, \dots, s$, at least one of u_i, v_i is zero. Set

$$\Lambda := \prod_{i=1}^{s} q_i^{v_i - u_i} - 1 = \frac{v}{u} - 1.$$

For $i = 1, \dots, s$, put $b_i = v_i - u_i$. Set $B = \max\{3, |b_1|, \dots, |b_s|\}$ and observe that

$$B \le 3 \log v. \tag{6.2}$$

By Theorem 2.9 there exists an effectively computable, absolute, real number C such that

$$\mathrm{v}_p(\Lambda) = \mathrm{v}_p(v-u) \le C^s \Big(\prod_{i=1}^{s} \log q_i \Big) \frac{p}{(\log p)^2} (\log B).$$

Combined with (6.2), this gives

$$\log |v-u|_p \ge -C^s \Big(\prod_{i=1}^{s} \log q_i \Big) \frac{p}{\log p} \log(3 \log v).$$

Taking the exponential of both sides, we get the assertion of the theorem. □

6.2. Waring's problem

Let $n \ge 2$ be an integer. Hilbert [228] proved that there exists an integer $s(n)$ such that every positive integer can be expressed as the sum of at most $s(n)$ positive integers, all of which being n-th powers. Let $g(n)$ denote the smallest integer with this property. Observe that the integer $2^n \lfloor (3/2)^n \rfloor - 1$ is less than 3^n, thus it can only be represented by using the n-th powers 1^n and 2^n. Since

$$2^n \lfloor (3/2)^n \rfloor - 1 = (\lfloor (3/2)^n \rfloor - 1) 2^n + (2^n - 1) 1^n,$$

we deduce the lower bound

$$g(n) \ge 2^n + \lfloor (3/2)^n \rfloor - 2. \tag{6.3}$$

It is known (see e.g. Chapter XXI of [220] for a review of such results) that equality holds in (6.3) when

$$2^n \{(3/2)^n\} + \lfloor (3/2)^n \rfloor \le 2^n. \tag{6.4}$$

Furthermore, if (6.4) fails, then

$$g(n) = 2^n + \lfloor (3/2)^n \rfloor + \lfloor (4/3)^n \rfloor - \theta,$$

where θ is equal to 2 or 3, according as the integer

$$\lfloor (4/3)^n \rfloor \cdot \lfloor (3/2)^n \rfloor + \lfloor (4/3)^n \rfloor + \lfloor (3/2)^n \rfloor$$

is equal to 2^n or is larger than 2^n. A quick check shows that, to prove that (6.4) holds for the integer n, it is sufficient to establish that

$$\|(3/2)^n\| \geq (3/4)^{n-1}. \tag{6.5}$$

The theory of linear forms in p-adic logarithms allows us to get an effective improvement of the trivial estimate $\|(3/2)^n\| \geq 2^{-n}$. This was first proved by Baker and Coates [34].

Theorem 6.2. *Let a and b be coprime integers with $a > b \geq 2$. Then, there exists an effectively computable positive real number δ, depending only on a and b, such that*

$$\left\| \left(\frac{a}{b}\right)^n \right\| \geq \frac{1}{2b^{(1-\delta)n}}, \quad \textit{for } n \geq 1.$$

Proof. Let n be a positive integer and A_n denote the nearest integer to $(a/b)^n$. Set

$$m_n := a^n - A_n b^n. \tag{6.6}$$

Let p be the smallest prime divisor of b. It follows from Theorems 2.8 (when a^n and m_n are multiplicatively dependent) and 2.12 that

$$n \leq \mathrm{v}_p(a^n - m_n) \ll_{a,b} (\log|2m_n|)\left(\log \frac{n}{\log|2m_n|}\right)^2,$$

giving that

$$n \ll_{a,b} \log|2m_n|.$$

This implies the existence of a positive real number δ, depending only on a and b, such that

$$2|m_n| \geq b^{\delta n}.$$

Combined with (6.6) we conclude that

$$\left\| \left(\frac{a}{b}\right)^n \right\| = \frac{|m_n|}{b^n} \geq \frac{1}{2b^{(1-\delta)n}}.$$

This completes the proof of the theorem. □

According to [111], in the case $\frac{a}{b} = \frac{3}{2}$, Theorem 6.2 holds with $\delta = 0.0005$, thus we are very far from proving (6.5) by means of the theory of linear forms in p-adic logarithms.

By using a totally different approach, Beukers [65] proved that $\|(3/2)^n\| \geq 2^{-9n/10}$ for $n > 5000$. This estimate has been subsequently refined by several authors, including Zudilin [453], who established that $\|(3/2)^n\| \geq 0.5803^n$ for every n greater than an effectively computable number. Note that Kubina and Wunderlich [246] have checked that Inequality (6.4) holds for n up to 471, 600, 000.

6.3. On the b-ary expansion of an algebraic number

Throughout this section, we denote by b an integer at least equal to 2. Let ξ be a real algebraic number of degree d at least 2. It follows from Liouville's Theorem A.5 that

$$\|q\xi\| \gg_\xi q^{-d+1}, \quad \text{for } q \geq 1. \tag{6.7}$$

When $d \geq 3$, we have established in Theorem 4.6 a slight improvement upon (6.7), namely that there exists an effectively computable positive number $\tau(\xi)$, depending only on ξ, such that

$$\|q\xi\| \gg_{\xi} q^{-d+1+\tau(\xi)}, \quad \text{for } q \geq 1.$$

Taking $q = b^n$, we get

$$\|b^n\xi\| \gg_{\xi} b^{-(d-1-\tau(\xi))n}, \quad \text{for } n \geq 1. \tag{6.8}$$

It is then natural to ask whether (6.8) also holds when ξ is of degree two. In this case, the first effective lower bound for $\|b^n\xi\|$ was given by Schinzel [354] in a landmark paper published in 1967, in which he developed the theory of linear forms in two p-adic logarithms, making completely explicit the bounds of Gelfond [199, 200]. He established that, for every integer $b \geq 2$ and every quadratic real number ξ, we have

$$\|b^n\xi\| > b^{-n} \exp\bigl(c(\xi, b)n^{1/7}\bigr), \quad \text{for } n \geq 1,$$

where $c(\xi, b)$ is a positive, effectively computable, real number depending only on ξ and b. By following his approach and using Theorem 2.12, Bennett and Bugeaud [51] extended (6.8) to quadratic real numbers.

Theorem 6.3. *For every integer $b \geq 2$ and every quadratic real number ξ, there exists a positive, effectively computable, real number $\tau(\xi, b)$, depending only on ξ and b, such that*

$$\|b^n\xi\| \gg_{\xi,b} b^{-(1-\tau(\xi,b))n}, \quad \textit{for } n \geq 1.$$

Unlike in (6.8), the real number $\tau(\xi, b)$ in Theorem 6.3 depends on the base b.

It follows from Ridout's Theorem A.8 that, for every integer $b \geq 2$ and every positive ε, every irrational algebraic number ξ satisfies

$$\|b^n\xi\| \gg^{\text{ineff}}_{\xi,b,\varepsilon} b^{-\varepsilon n}.$$

The implicit numerical constant is, however, not effectively computable.

Proof of Theorem 6.3. We follow Schinzel's argument and the proof of Theorem 1.2 of [51]. It is sufficient to treat the case $\xi = \sqrt{a}$, where $a \geq 2$ is a non-square integer. Let x, n be positive integers with $|x - \sqrt{a}b^n| \leq 1$. Write

$$x^2 - ab^{2n} = (x + \sqrt{a}b^n) \cdot (x - \sqrt{a}b^n) =: \Delta.$$

Let η denote the fundamental unit (see Appendix C) of the quadratic field generated by $\sqrt{a}$. Write

$$x - \sqrt{a}b^n = \delta\eta^m,$$

where δ in $\mathbb{Q}(\sqrt{a})$ and the integer m are such that

$$|\Delta|^{1/2} \cdot \eta^{-1/2} < |\delta| \leq |\Delta|^{1/2} \cdot \eta^{1/2}, \quad \delta\delta^{\sigma} = \Delta. \tag{6.9}$$

Here and below, δ^{σ} denotes the Galois conjugate of δ. Observe that $m \leq 0$ and

$$(x^2 - ab^{2n}) - (x - \sqrt{a}b^n)^2 = \Delta - \delta^2\eta^{2m} = 2(\sqrt{a}b^n x - ab^{2n}). \tag{6.10}$$

Let us factor $b = q_1^{\ell_1} \cdots q_s^{\ell_s}$ as a product of powers of distinct prime numbers. Choose j so that $\ell_j = \max\{\ell_1, \ldots, \ell_s\}$, and put $p = q_j$ and $\ell = \ell_j$. Set $M := \max\{2, |m|\}$. Since $|\delta^\sigma| \ge \eta^{-1/2}$ and

$$|\delta^\sigma \eta^{-m}| = |x + \sqrt{a} b^n| \le 1 + 2\sqrt{a} b^n \ll_a b^n,$$

we get

$$M \ll_a n \log b. \tag{6.11}$$

If $m = 0$, then we immediately derive that $n \ll_{a,b} \log |2\Delta|$. If $m < 0$ and $|\Delta| = 1$, then $\delta = \pm 1$ and we deduce from (6.10), (6.11), and Theorem 2.8 that

$$n \le n\ell \le \mathrm{v}_p(\eta^{2m} \pm 1) \le \mathrm{v}_p(\eta^{4m} - 1) \ll_{a,p} \log M \ll_{a,b} \log n,$$

which gives an effective upper bound for n, depending only on a and b.

We assume now that $|\Delta| \ge 2$ and $m < 0$. We wish to bound

$$\mathrm{v}_p(\Delta - \delta^2 \eta^{2m}) = \mathrm{v}_p\Big(\frac{\delta^\sigma}{\delta} - \eta^{2m}\Big) + \mathrm{v}_p(\delta^2)$$

from above. It follows from (6.9) that $\eta^{-1} \le |\delta/\delta^\sigma| \le \eta$. Since $\delta\Delta/\delta^\sigma$ is an algebraic integer, the height of δ^σ/δ is $\ll_a \log |\Delta|$. By Theorem 2.12, we get

$$\mathrm{v}_p\Big(\frac{\delta^\sigma}{\delta} - \eta^{2m}\Big) \ll_{a,p} (\log |\Delta|)\Big(\log\Big(2 + \frac{M}{\log |\Delta|}\Big)\Big)^2. \tag{6.12}$$

On the other hand, we derive from (6.10) that

$$\mathrm{v}_p\Big(\frac{\delta^\sigma}{\delta} - \eta^{2m}\Big) \ge n\ell - \mathrm{v}_p(\delta^2),$$

while $\mathrm{v}_p(\delta) \ll_{a,b} \log |\Delta|$, by (6.9). Combined with (6.11) and (6.12), this gives

$$\begin{aligned} n \le n\ell &\ll_{a,p} (\log |\Delta|)\Big(\log\Big(2 + \frac{n(\log b)}{\log |\Delta|}\Big)\Big)^2 + \log |\Delta| \\ &\ll_{a,p} (\log |\Delta|)\Big(\log\Big(2 + \frac{n(\log b)}{\log |\Delta|}\Big)\Big)^2, \end{aligned}$$

whence

$$n \ll_{a,b} \log |\Delta|.$$

Taking for x the nearest integer to $\sqrt{a} b^n$, all this proves the existence of an effectively computable, positive, real number κ, depending only on a and b, such that

$$\|b^n \sqrt{a}\| = |x - \sqrt{a} b^n| \ge \frac{|\Delta|}{2\sqrt{a} b^n + 1} \ge \frac{b^{\kappa n}}{2\sqrt{a} b^n + 1}.$$

This concludes the proof of the theorem. □

6.4. Repunits and perfect powers

We continue this chapter with a special case of an equation already discussed in Corollary 3.11. In the proof of the next theorem, the use of estimates for linear forms in p-adic logarithms yields better numerical upper bounds than the use of estimates for linear forms in complex logarithms. A *repunit* is an integer all of whose decimal digits are 1.

Theorem 6.4. *The Diophantine equation*

$$\frac{10^n - 1}{10 - 1} = y^q \tag{6.13}$$

has no solution in integers n, y, q with $n \geq 2$ and $q \geq 2$. Said differently, no repunit greater than 1 is a perfect power.

In 1976, Shorey and Tijdeman [375] established that (6.13) has only finitely many solutions and solved it for $q < 23$. Its full resolution was completed in 1999 in [132]; see also [133, 135]. We point out that (6.13) has a solution for every $q \geq 2$ given by $10^1 = 9 \cdot 1^q + 1$, which makes its resolution a difficult problem (a naïve sieve for fixed q does not yield any contradiction). There are much similarities between the proofs of Theorem 6.4 and Theorem 3.12.

Outline of the proof of Theorem 6.4. Rewriting (6.13) in the form

$$9y^q 10^{-n} - 1 = -10^{-n},$$

we can obtain an upper bound for q by using estimates for linear forms in three complex logarithms; see Section 3.7 for details. Here, we rather use the fact that the binary recurrence sequence $(\frac{10^m-1}{9})_{m\geq 0}$ has a dominant root for the 5-adic absolute value in order to obtain a much sharper bound for q, which follows from an estimate for linear forms in two 5-adic logarithms. Namely, we consider the 5-adic valuation of

$$10^n = 9y^q + 1.$$

On the one hand, it is trivially equal to n. On the other hand, Theorem 2.12 allows us to bound $\mathrm{v}_5(9y^q + 1)$ from above.

Observe that $3^h + 1$ is congruent to 2 or 4 modulo 8 for $h \geq 1$. Thus, if we have $10^n = 9y^q + 1$ with y being a power of 3, then n must be at most equal to 2 and we conclude that the only solution is given by $y = 1$. Hence, we may assume that 9 and y are multiplicatively independent and we derive from Theorem 2.12 that

$$n = \mathrm{v}_5(9y^q + 1) \ll (\log y)(\log q)^2,$$

where the constant implied by $\ll$ is reasonably small. Combined with the obvious bound $y^q \leq 10^n$, we derive that

$$q \log y \ll (\log y)(\log q)^2 \ ,$$

and we get at once an upper bound for q. This upper bound is much smaller than the one which can be derived from estimates for three complex logarithms. By using the full force of the main result of [129], the authors of [132] proved that $q \leq 2063$; thus, since q may clearly be assumed to be prime, they replaced Equation (6.13) in three unknowns by about three hundred equations in only two unknowns.

Therefore, we may assume that q is a fixed prime number in (6.13). Taking into account the result of Shorey and Tijdeman [376] mentioned above, we use congruences for each value of the prime number q in the range $23 \leq q \leq 2063$. The idea goes as follows. Consider a prime number ℓ of the form $\ell = hq + 1$ for some even integer h. Then, $(y^q)^h$ is congruent to 0 or to 1 modulo ℓ, giving us that y^q can take at most $h + 1$ different values modulo ℓ. Since $10^n = 9y^q + 1$, we deduce that n takes at most $h + 1$ different values modulo $\ell - 1$, hence at most $h + 1$ different values modulo q, since q divides $\ell - 1$. Combining the information given by a few different prime numbers ℓ congruent to 1 modulo q, we conclude after some computation that n must be congruent to 1 modulo q.

Hence, there exists a positive integer ν such that $n = \nu q + 1$ and we get the equality

$$10 \cdot (10^\nu)^q - 9y^q = 1.$$

This means that $X = 10^\nu, Y = y$ is a solution of the Thue equation

$$10X^q - 9Y^q = 1,$$

which has already been considered in Section 5.3. By Theorem 5.5, this equation has no solution with $Y \geq 2$. We conclude that $y = 1$, $\nu = 0$, and $n = 1$, which has been excluded. This completes the outline of the proof of the theorem. □

6.5. Perfect powers with few binary digits

Theorem 3.16 implies that a large integral power of 3 cannot have too few digits 1 in its binary representation. In this section, we study a more general question and ask whether an arbitrarily large perfect power can have only a bounded number of digits 1 in its binary representation. For a given integer $x \geq 2$, equations of the form

$$x^a + x^b + x^c + 1 = y^q,$$

where $a > b > c > 0$, $q \geq 2$, $y \geq 2$ are unknown integers, have been considered in an handful of papers, including [48, 49, 52–54, 159, 274, 409]. We reproduce a result established in [53].

Theorem 6.5. *If the integers a, b, y, q satisfy $a > b \geq 1$, $q \geq 2$, and*

$$2^a + 2^b + 1 = y^q, \tag{6.14}$$

then $(a, b, y, q) = (5, 4, 7, 2), (9, 4, 23, 2), (6, 4, 3, 4)$, or $(a, b, y, q) = (2t, t + 1, 2^t + 1, 2)$, for some integer $t \geq 2$. If there exist positive integers a, b, c, y, and q such that $a > b > c \geq 1$ and

$$2^a + 2^b + 2^c + 1 = y^q, \tag{6.15}$$

then $q \leq 4$.

It is clear from the proof of Theorem 6.5 that the $+1$ in (6.14) and (6.15) is crucial: we do not know how to prove, for instance, whether or not the equation $2^a + 2^b + 7 = y^q$ has no solution when q is sufficiently large.

A crucial ingredient in the proof of the second statement of the theorem is the refined estimate for p-adic linear forms in logarithms, given in Theorem 2.13, in the special case where the rational numbers involved are p-adically very close to 1.

Outline of the proof of Theorem 6.5. We content ourselves to explain how to derive an effectively computable upper bound for q, assuming that q is an odd prime. We do not discuss the final sieve, performed for fixed values of q. We first show that, when q is sufficiently large, equations (6.14) and (6.15) have no solutions satisfying $a \geq 2b$.

Let (a, b, y, q) (*resp.,* (a, b, c, y, q)) be a solution of (6.14) (*resp.,* of (6.15)) with $a > b \geq 1$ (*resp., $a > b > c \geq 1$*). Observe that

$$a \ll q(\log y) \ll a. \tag{6.16}$$

Assume that $a \geq 2b$. Then, we have

$$|y^q 2^{-a} - 1| < 2^{2-(a-b)} \leq 2^{2-a/2}. \tag{6.17}$$

Since y is odd, the integers 2 and y are multiplicatively independent and (6.16) and Theorem 2.3 then give that

$$\begin{aligned}\log|y^q 2^{-a} - 1| &\gg -(\log y)\left(\log\Bigl(q + \frac{a}{\log y}\Bigr)\right)^2 \\ &\gg -(\log y)\,(\log q)^2 \gg -a\,\frac{(\log q)^2}{q}.\end{aligned}$$

Combined with (6.17), we immediately obtain the upper bound

$$q \ll (\log q)^2,$$

and we conclude that $q \ll 1$ for every solution (a, b, y, q) (*resp.,* (a, b, c, y, q)) of (6.14) (*resp.,* of (6.15)) with $a > b \geq 1$ (*resp., $a > b > c \geq 1$*) and $a \geq 2b$.

Assume that $2b > a$.

First, consider Equation (6.14). It is immediate that 2^b divides $y^q - 1$. Since y and q are odd, $1 + y + \cdots + y^{q-1}$ is also odd, hence 2^b divides $y - 1$ and $y \geq 2^b + 1$. Thus, we get

$$2^a + 2^b + 1 \geq (2^b + 1)^q > 2^{bq} + 2^b + 1$$

and derive the inequality

$$2b \leq bq < a.$$

This shows that (6.14) has no solution with $2b > a$ for any odd prime number q.

Secondly, consider Equation (6.15). The same argument implies that 2^c divides $y - 1$. Note that

$$b = \mathrm{v}_2(2^a + 2^b) = \mathrm{v}_2(y^q - (2^c + 1)). \tag{6.18}$$

If $2^c + 1$ and y are multiplicatively dependent, then, after a little work, we find that

$$\text{either} \quad 2^a + 2^b + 9 = 3^q, \quad \text{or} \quad 2^a + 2^b + C = C^q,$$

where $C = 2^c + 1$ and $c \neq 3$. In the first case, arguing modulo 4 contradicts our assumption that q is odd. In the second case, we write $q - 1 = 2^k Q$ where Q is odd, so that $\mathrm{v}_2(C^{2^k} - 1) = b$. By expanding via the binomial theorem, it is easy to see that $\mathrm{v}_2(C^{2^k} - 1) \leq c + k + 2$, whereby $b \leq c + k + 2$. Since $2^a + 2^b + 2^c + 1 = (2^c + 1)^q$ implies that $a \geq cq$, we thus have

$$b \leq c + k + 2 \leq \frac{a}{q} + \frac{\log q}{\log 2} + 2 \leq \frac{a}{q} + \frac{\log a}{\log 2} + 2.$$

Since $2b > a$, we deduce that $q \ll 1$.

Thus, we assume that $2^c + 1$ and y are multiplicatively independent. If $c = 1$ or 2, then we derive from Theorem 2.12 upper bounds for $\mathrm{v}_2(y^q - 3)$ and $\mathrm{v}_2(y^q - 5)$, which, by (6.18), give in both cases

$$b \ll (\log y)\,(\log q)^2.$$

Since $b > \frac{a}{2}$, it then follows from (6.16) that $q \ll 1$. If $c \geq 3$, then we apply Theorem 2.13 with the parameter $E = \mathrm{v}_2((2^c + 1) - 1) = c$ and, recalling that $\mathrm{v}_2(y - 1) \geq c$, we get $y > 2^c$ and

$$\mathrm{v}_2(y^q - (2^c + 1)) \ll \frac{(\log(2^c + 1))\,(\log y)}{c^3} \max\{\log q, c\}^2 \ll (\log y)\,(\log q)^2.$$

Combined with (6.16), (6.18), and $b > \frac{a}{2}$, this gives $q \ll 1$. This shows that (6.15) has no solutions with $2b \geq a$ when q is sufficiently large. We have established that every solution to (6.14) or (6.15) satisfies $q \ll 1$. □

6.6. The S-unit equation

Let K be an algebraic number field and S be a finite set of places on K containing the set of infinite places. An algebraic number x in K is an S-unit if, by definition, $|x|_v = 1$ for every place v not in S. The S-unit equation is a natural extension of the unit equation studied in Section 4.2.

Theorem 6.6. *Let K be an algebraic number field of degree d and discriminant D_K. Let S be a finite set of places on K containing the infinite places. Let α, β be non-zero elements of K. The equation*

$$\alpha x + \beta y = 1, \quad \text{in } S\text{-units } x, y \text{ in } K, \tag{6.19}$$

has only finitely many solutions, and all of them satisfy

$$\max\{h(x), h(y)\} \ll_{d, D_K, S} \max\{h(\alpha), h(\beta), 1\}. \tag{6.20}$$

When S is the set of infinite places, then (6.19) is an (ordinary) unit equation. The first explicit version of Theorem 6.6 was established by Győry [211]. For more recent explicit versions, generalisations, and applications, see [124, 182–184, 217].

Proof. Let x, y be a solution to (6.19). We assume that $h(x) \geq h(y)$. Let s be the cardinality of S. The case $s = 1$ being trivial, we assume that $s \geq 2$. Let $\{\eta_1, \dots, \eta_{s-1}\}$ be a fundamental system of S-units in K satisfying the properties specified in Lemma C.4. Then we can write

$$y = \zeta \eta_1^{b_1} \dots \eta_{s-1}^{b_{s-1}}, \tag{6.21}$$

where ζ is a root of unity in K and $b_1, \dots, b_{s-1}$ are rational integers.

Put $B = \max\{|b_1|, \dots, |b_{s-1}|, 3\}$ and let $v_1, \dots, v_s$ denote non-equivalent places in S. Then (6.21) implies

$$\log |y|_{v_j} = \sum_{i=1}^{s-1} b_i \log |\eta_i|_{v_j}, \quad j = 1, \dots, s-1.$$

Using Cramer's rule and the definition of the height, we get from (6.21) and Lemma C.4 that

$$B \ll_{d,D_K,S} h(y) \ll_{d,D_K,S} B. \tag{6.22}$$

Let v be a place in S for which $|x|_v$ is minimal. It then follows from Definition B.4 that

$$h(x) = h\Big(\frac{1}{x}\Big) \leq -\log |x|_v. \tag{6.23}$$

Assume, without any loss of generality, that $h(x) \geq 2dh(\alpha)$. Then, we deduce from (6.22) and (6.23) that

$$\log |\alpha x|_v \leq dh(\alpha) - h(x) \leq -\frac{h(x)}{2} \leq -\frac{h(y)}{2} \ll_{d,D_K,S} (-B). \tag{6.24}$$

Setting $\alpha_s = \zeta\beta$ and $b_s = 1$, we get from (6.19) that

$$|\alpha x|_v = |\eta_1^{b_1} \dots \eta_{s-1}^{b_{s-1}} \alpha_s^{b_s} - 1|_v. \tag{6.25}$$

We shall derive a lower bound for $|\alpha x|_v$. Set $H := \exp(\max\{h(\alpha), h(\beta), 1\})$.

First assume that the place v is infinite. We can proceed as in the proof of Theorem 4.3, but we rather apply Theorem 2.2 to (6.25). Combined with Lemma C.4, we derive that

$$\log |\alpha x|_v \gg_{d,D_K,S} \Big(-\log H \, \log\Big(\frac{B}{\log H}\Big)\Big). \tag{6.26}$$

Hence it follows from (6.26) and (6.24) that

$$\frac{B}{\log H} \ll_{d,D_K,S} \log\Big(\frac{B}{\log H}\Big).$$

This gives

$$B \ll_{d,D_K,S} \log H.$$

Next, assume that the place v is finite. Let p be the prime number below v. We apply the last assertion of Theorem 2.11 with $n = s$ in the case $b_s = 1$ to get that either

$$B \ll_{d,D_K,S} 1$$

or

$$\log |\eta_1^{b_1} \dots \eta_{s-1}^{b_{s-1}} \alpha_s^{b_s} - 1|_v \gg_{d,p} \left(-\mathrm{v}_p(\eta_1^{b_1} \dots \eta_{s-1}^{b_{s-1}} \alpha_s^{b_s} - 1)\right)$$
$$\gg_{d,D_K,S} \Big(-\log H \, \log\Big(\frac{B}{\log H}\Big)\Big).$$

By (6.24) and (6.25), we have in both cases

$$B \ll_{d,D_K,S} \log H. \tag{6.27}$$

Since

$$h(x) \le h(y) + 2\log H + 2\log 2,$$

we deduce from (6.22) and (6.27) that (6.20) holds. It then follows from Northcott's Theorem B.7 that (6.19) has only finitely many solutions. □

6.7. The Thue–Mahler equation and other classical equations

In 1933 Mahler [279] established the finiteness of the number of coprime *rational* solutions to the Thue equation, whose denominators are composed only of prime numbers from a given, finite set. The theory of linear forms in logarithms allows us to get effective upper bounds for the size of these solutions and to prove the following result, which was established under a weaker form by Coates [150].

Theorem 6.7. *Let s be a positive integer and $q_1, \dots, q_s$ distinct prime numbers. Let $F(X,Y)$ be an homogeneous polynomial with integer coefficients such that $F(X,1)$ has at least three distinct roots. Let m be a non-zero integer. The Diophantine equation*

$$F(x,y) = mq_1^{z_1} \dots q_s^{z_s}, \quad \text{in integers } x, y, z_1, \dots, z_s \text{ with } \gcd(x,y) = 1 \text{ and } z_1, \dots, z_s \ge 0, \tag{6.28}$$

has only finitely many solutions, and all of these can be effectively determined. Moreover, there exists an explicitely computable real number C, depending only on $F, q_1, \dots, q_s$, such that every solution of (6.28) *satisfies*

$$\max\{|x|, |y|, q_1^{z_1} \dots q_s^{z_s}\} \le |2m|^C.$$

Equation (6.28) is called the Thue–Mahler equation. For explicit versions, further references, applications, and generalisations to norm form and decomposable form equations, see e.g. [125, 212, 217] and [182, 183].

There are similar p-adic extensions of the superelliptic equation, the hyperelliptic equation, and further classical equations; see e.g. [61, 101, 376, 386]. We are able to establish effective upper bounds for the size of the solutions to these equations in rational numbers whose denominators are composed only of prime numbers from a given, finite set. We state below extensions of Theorems 4.7 and 4.9, established (under a slightly different formulation and over algebraic number fields) in [376].

Theorem 6.8. *Let S be a finite, non-empty set of prime numbers. Let $f(X)$ be an integer polynomial of degree m without multiple roots, and let n be an integer. Assume that $m \geq 2$, $n \geq 2$, and $mn \geq 6$. Let t be a non-zero integer. If the rational numbers x, y satisfy*

$$f(x) = ty^n$$

and if the denominator of x is composed only of prime numbers from S, then

$$\max\{h(x), h(y)\} \ll_{f,t,n,S} 1.$$

Theorem 6.9. *Let S be a finite, non-empty set of prime numbers. Let $f(X, Z)$ be a homogeneous, integer polynomial of degree $n \geq 2$ without multiple roots. Set $m_0 = 3$ if $n = 2$ and $m_0 = 2$ otherwise. If there exist integers x, y, z, t, m with $m \geq m_0$, $|y| \geq 2$, $\gcd(x, z) = 1$, such that tz is composed only of prime numbers from S and*

$$f(x, z) = ty^m,$$

then $\max\{|x|, |y|, |t|, |z|, m\} \ll_{f,S} 1$.

Lower bounds for the greatest prime factor of quantities of the form $ax^m + by^n$ follow from explicit versions of Theorems 6.8 and 6.9.

Theorem 6.10. *Let a, b, m, n be non-zero integers such that $m \geq 2$, $n \geq 2$, and $mn \geq 6$. For any coprime integers x, y, setting $X := \max\{|x|, |y|, 16\}$, we have*

$$P[ax^m + by^n] \gg_{a,b,m,n} \log\log X,$$

and, in the special case $m = n$,

$$P[ax^n + by^n] \gg_{a,b,n} \log\log X \, \frac{\log\log\log X}{\log\log\log\log X}.$$

Theorem 6.11. *Let a, b, x, y, and n be integers satisfying*

$$ab \neq 0, \ |x| > 1, \quad y \neq 0, \quad \gcd(ax, by) = 1, \quad \textit{and} \quad n \geq 2.$$

Then, for any integer $m \geq 2$, we have

$$P[ax^m + by^n] \gg_{a,b,n} \log m.$$

Theorems 6.10 and 6.11, along with more general statements, have been established in [106, 108, 110, 122, 217, 221].

6.8. Perfect powers in binary recurrence sequences

In Section 3.7 we established that, under the dominant root condition, a recurrence sequence of integers does not contain any integer of the form y^q, where $|y| \geq 2$ and q is a sufficiently large prime number. In the case of binary recurrence sequences, the dominant root condition can be removed. The next result was proved independently by Pethő [323] and Shorey and Stewart [372].

THEOREM 6.12. *Let* $\mathbf{u} = (u_n)_{n\geq 0}$ *be a non-degenerate binary recurrence sequence of integers. Then, the equation*

$$u_n = y^q, \tag{6.29}$$

in integers n, y, q *with* $|y| \geq 2$ *and* q *a prime number, implies that*

$$\max\{n, |y|, q\} \ll_{\mathbf{u}} 1.$$

Proof. First, we establish that q is bounded. Write

$$u_n = a\alpha^n + b\beta^n, \quad n \geq 0, \quad \text{where } a = \frac{u_0\beta - u_1}{\beta - \alpha},\ b = \frac{u_1 - u_0\alpha}{\beta - \alpha},$$

and α, β are roots of a monic, integer quadratic polynomial. If α and β are real numbers, then either $|\alpha| > |\beta|$, or $|\beta| > |\alpha|$ and we apply Theorem 3.10 to conclude that $q \ll_{\mathbf{u}} 1$. Thus, we may assume that α and β are complex non-real. In particular, $|\alpha| = |\beta|$ and α is the Galois conjugate of β.

Observe that α/β and β/α are conjugate algebraic numbers of degree two and of absolute value one. Since α/β is not a root of unity and any unit in $\mathbb{Q}(\alpha)$ is a root of unity, neither α/β nor β/α are algebraic integers. Thus, there exists a prime number p, depending only on $\mathbf{u}$, such that $\mathrm{v}_p(\alpha/\beta)$ or $\mathrm{v}_p(\beta/\alpha)$ is positive. Without any loss of generality, we assume that $\mathrm{v}_p(\alpha/\beta)$ is positive. Let n be a large integer, q a prime number greater than p, and y an integer such that $|y| \geq 2$ and (6.29) holds. Then, we have

$$\mathrm{v}_p(y^q b^{-1}\beta^{-n} - 1) = \mathrm{v}_p\Big(\frac{a}{b}\Big) + n\mathrm{v}_p\Big(\frac{\alpha}{\beta}\Big) \tag{6.30}$$

and

$$q \log y \ll_{\mathbf{u}} n. \tag{6.31}$$

Since $\mathrm{v}_p(q) = 0$, we apply Theorem 2.11 with $n = 3$, $B_3 = b_3 = q$, and $\delta = \frac{1}{2}$, to get that

$$\mathrm{v}_p(y^q b^{-1}\beta^{-n} - 1) \ll_{\mathbf{u}} \max\Big\{(\log y)(\log q), \frac{n}{q}\Big\}.$$

Combined with (6.30) this gives

$$n \ll_{\mathbf{u}} \max\Big\{(\log y)(\log q), \frac{n}{q}\Big\}. \tag{6.32}$$

It then follows from (6.31) and (6.32) that

$$q \ll_{\mathbf{u}} 1.$$

It remains for us to prove that, for any fixed value of q at least 2, Equation (6.29) has only finitely many solutions. Write

$$v_n = (\alpha - \beta)\,(a\alpha^n - b\beta^n), \quad n \geq 0.$$

Clearly, we have

$$(\alpha - \beta)^2 u_n^2 - v_n^2 = 4ab(\alpha - \beta)^2(\alpha\beta)^n.$$

Observe that $(\alpha - \beta)^2$, $\alpha\beta$, and $4ab(\alpha - \beta)^2$ are rational integers. If (6.29) holds, then there exists an integer r with $0 \le r < 2q$ such that the hyperelliptic equation

$$(\alpha - \beta)^2 X^{2q} - 4ab(\alpha - \beta)^2 (\alpha\beta)^r = Y^2$$

has a solution in rational numbers X, Y, with X being an S-unit, where S is the set of prime divisors of $\alpha\beta$. Since the polynomial $(\alpha - \beta)^2 X^{2q} - C$ has $2q$ distinct complex roots for any non-zero integer C, it follows from Theorem 6.8 that all the solutions of each of these $2q$ hyperelliptic equations satisfy $\max\{h(X), h(Y)\} \ll_{\mathbf{u}} 1$. This completes the proof of the theorem. □

6.9. Perfect powers as sum of two integral S-units

Let S denote a finite, non-empty set of prime numbers. We establish below that the sum of two integral S-units cannot be an arbitrarily large power of an integer greater than or equal to 2.

Theorem 6.13. *Let S be a finite, non-empty set of prime numbers. If there exist integers x, y, z, ℓ with ℓ prime, x, y coprime and composed only of prime numbers from S, $|z| \ge 2$, and such that*

$$x + y = z^\ell,$$

then

$$\max\{|x|, |y|, |z|, \ell\} \ll_S 1.$$

Proof. This is (a particular case) of Theorem 9.2 of [376]; see also [50]. Let $q_1, \dots, q_s$ denote the elements of S. Assume there exist non-negative integers $u_1, \dots, u_s, v_1, \dots, v_s$, a prime number ℓ, and an integer z with $|z| \ge 2$, such that

$$q_1^{u_1} \dots q_s^{u_s} \pm q_1^{v_1} \dots q_s^{v_s} = z^\ell \tag{6.33}$$

and $\min\{u_j, v_j\} = 0$ for $j = 1, \dots, s$. Set $M := \max\{u_1, \dots, u_s, v_1, \dots, v_s\}$. Assume that ℓ exceeds $q_1, \dots, q_s$. Since ℓ is prime, we have $\mathrm{v}_{q_j}(\ell) = 0$ for $j = 1, \dots, s$.

Assume that $u_1 \ge 1$. By applying Theorem 2.11 with

$$\alpha_n = z, \quad b_n = \ell, \quad \{\alpha_1, \dots, \alpha_{n-1}\} = \{q_j : v_j \ge 1, 1 \le j \le s\}, \quad p = q_1, \quad B_n = \ell,$$

and $\delta = \frac{1}{2}$, we get

$$u_1 \ll_S \max\Big\{(\log|z|)(\log\ell), \frac{M}{\ell}\Big\}.$$

Arguing similarly to bound $u_2, \dots, u_s, v_1, \dots, v_s$, we obtain

$$M = \max\{u_1, \dots, u_s, v_1, \dots, v_s\} \ll_S \max\Big\{(\log|z|)(\log\ell), \frac{M}{\ell}\Big\},$$

and, consequently,

$$\ell \ll_S 1 \quad \text{or} \quad M \ll_S (\log|z|)(\log\ell). \tag{6.34}$$

However, we deduce from (6.33) that

$$\ell \log|z| \ll_S M.$$

We conclude from (6.34) that $\ell \ll_S \log\ell$ holds in both cases, thus $\ell \ll_S 1$. The theorem then follows from Theorem 6.7. We leave the details to the reader. □

6.10. On the digital representation of integral S-units

Let S be a finite set of prime numbers and b, k integers at least equal to 2. The next result, proved by Bugeaud and Kaneko [128], shows that every sufficiently large integer which is divisible only by prime numbers in S, and is not a multiple of b, has more than k non-zero digits in its representation in base b.

Theorem 6.14. *Let $b \ge 2$ be an integer. Let S be a finite, non-empty set of prime numbers. Then, there exist effectively computable positive integers n_0 and C, depending only on b and S, such that any integral S-unit $n \ge n_0$ which is not divisible by b has more than*

$$\frac{\log\log n}{C + \log\log\log n}$$

non-zero digits in its representation in base b.

Let $a \ge 2, b \ge 2$ be coprime integers. By taking for S the set of prime divisors of a, Theorem 6.14 allows us to recover a consequence of Theorem 3.16 in the particular case where m is a power of a (for the case where a and b are multiplicatively independent and not coprime, the proof of Theorem 6.14 can be easily adapted) and both proofs are different.

Proof. Let $N > b$ be an integral S-unit and k the number of non-zero digits in its representation in base b. We assume that b does not divide N, thus $k \ge 2$ and we write

$$N =: d_k b^{n_k} + \cdots + d_2 b^{n_2} + d_1 b^{n_1},$$

where

$$n_k > \cdots > n_2 > n_1 = 0, \quad d_1, \ldots, d_k \in \{1, \ldots, b-1\}.$$

Let s be the cardinality of S and $q_1, \ldots, q_s$ its elements written in increasing order. There exist non-negative integers $r_1, \ldots, r_s$ such that

$$N = q_1^{r_1} \cdots q_s^{r_s}.$$

Observe that

$$b^{n_k} \le N < b^{n_k+1}. \tag{6.35}$$

First we assume that $n_k \ge 2n_{k-1}$. This covers the case $k = 2$. Since

$$\Lambda_a := \left| \Big(\prod_{i=1}^{s} q_i^{r_i} \Big) d_k^{-1} b^{-n_k} - 1 \right| = d_k^{-1} b^{-n_k} \sum_{h=1}^{k-1} d_h b^{n_h} \le b^{1+n_{k-1}-n_k} \le b^{-(n_k-2)/2},$$

we get

$$\log \Lambda_a \le -\Big(\frac{n_k}{2} - 1\Big) \log b. \tag{6.36}$$

By using the inequality

$$r_j \log q_j \le (n_k + 1) \log b, \quad \text{for } j = 1, \ldots, s, \tag{6.37}$$

we deduce from Theorem 2.2 that

$$\log \Lambda_a \gg_{b,S} (-\log n_k). \tag{6.38}$$

Combining (6.35), (6.36), and (6.38), we obtain

$$N \ll_{b,S} 1.$$

Now, we assume that $n_k < 2n_{k-1}$. In particular, we have $k \geq 3$. If there exists an integer j with $1 \leq j \leq k-3$ and $n_{1+j} \geq n_k^{j/(k-2)}$, then put

$$\ell := \min \{ j : 1 \leq j \leq k-3,\ n_{1+j} \geq n_k^{j/(k-2)} \}.$$

Otherwise, set $\ell := k-2$. We see that, by construction,

$$n_{\ell+1} \geq \frac{1}{2} n_k^{\ell/(k-2)} \quad \text{and} \quad n_\ell \leq n_k^{(\ell-1)/(k-2)}. \tag{6.39}$$

Let p be the smallest prime divisor of b. Put

$$\Lambda_u := \Big(\prod_{i=1}^{s} q_i^{r_i}\Big)\Big(\sum_{h=1}^{\ell} d_h b^{n_h}\Big)^{-1} - 1 = \Big(\sum_{h=\ell+1}^{k} d_h b^{n_h}\Big)\Big(\sum_{h=1}^{\ell} d_h b^{n_h}\Big)^{-1}.$$

We get by (6.39) and (6.35) that

$$\mathrm{v}_p(\Lambda_u) \geq n_{\ell+1} - \frac{\log b^{1+n_\ell}}{\log p} \geq \frac{1}{4} n_k^{\ell/(k-2)}, \tag{6.40}$$

if $N \gg_{b,S} 1$. We deduce from Theorem 2.9, (6.39), and (6.37) that

$$\mathrm{v}_p(\Lambda_u) \ll_{b,S} n_k^{(\ell-1)/(k-2)} \log n_k. \tag{6.41}$$

By combining (6.40) and (6.41), we get

$$n_k^{1/(k-2)} \ll_{b,S} (k-2) \log\big(n_k^{1/(k-2)}\big),$$

which, by (6.35), establishes the conclusion of Theorem 6.14. □

6.11. Exercises

EXERCISE 6.1. Let S denote a finite set of prime numbers and $(x_j)_{j \geq 1}$ the increasing sequence of all positive integers whose prime factors belong to S. Let h, j be integers with $1 \leq h < j$ and $j \geq 3$. If x_h and x_j are coprime, establish that

$$P[x_h + x_j] \gg_S (\log x_j)^{1/2} (\log \log x_j)^{1/2}.$$

Exercise 6.2 (see Lemma 4.1 of [376]). Let $f(X)$ be a non-constant polynomial with algebraic coefficients and α a non-zero algebraic number. Apply Theorems 2.8 and 2.1 to show that the equation

$$f(m)\alpha^m = f(n)\alpha^n, \quad m > n > 0,$$

implies that $m \ll_{f,\alpha} 1$.

Exercise 6.3. Let $P \geq 2$ be an integer and α an irrational, algebraic number. Prove that there exists an effectively computable real number C, depending only on α and P, such that, for every rational number $\frac{p}{q}$ with $q \geq 2$ and $P[pq] \leq P$, we have

$$\left|\alpha - \frac{p}{q}\right| \geq (\log q)^{-C}.$$

Compare with Ridout's Theorem A.8.

Exercise 6.4 (see [102, 103]). Consider the Diophantine equation $x^2 - 2^m = y^n$ with x and y coprime and $n > 2$. Prove that m and n must be odd. Factor the left-hand side in $\mathbb{Z}[\sqrt{2}]$ and combine the use of estimates for linear forms in two complex and in two 2-adic logarithms to prove that n is bounded. Let p be an odd prime number. Show how the same method applies to the Diophantine equation $x^2 - p^m = y^n$ to bound the exponent n.

Exercise 6.5 (see [373]). Establish the p-adic analogue of Theorem 3.10, that is, its analogue for recurrence sequences having a dominant root for some p-adic absolute value (see the proof of Theorem 6.4).

Exercise 6.6. Recall that $(p_k)_{k\geq 1}$ denotes the increasing sequence of prime numbers. According to Guy [206, Section A2], Erdős and Stewart conjectured that the only solutions of the equation

$$n! + 1 = p_k^a p_{k+1}^b, \quad \text{for some } a, b \geq 0 \text{ and } p_{k-1} \leq n < p_k, \tag{6.42}$$

are obtained for $n \leq 5$. This was confirmed by Luca [273]. Use linear forms in two 2-adic logarithms to show that every solution (a, b, k, n) of (6.42) satisfies $n \ll 1$.

Exercise 6.7 (see [118]). Let S be a finite, non-empty set of prime numbers. For a positive integer n, let $[n]_S$ denote the greatest divisor of n, all of whose prime factors are in S. Let $b \geq 2$ be an integer and $(u_n)_{n\geq 1}$ the increasing sequence of all the positive integers which are not divisible by b and have at most three non-zero digits in their representation in base b. Use estimates for complex and p-adic linear forms in logarithms to prove that there exist effectively computable positive numbers c and n_0, depending only on S and b, such that $[u_n]_S < (u_n)^{1-c}$, for every $n > n_0$.

Exercise 6.8 (see [333]). Let $q_1, \ldots, q_s$ be distinct prime numbers, and denote by P their maximum. Combine Theorems 2.3 and 2.12 to show that, for every solution to the Diophantine equation

$$x^2 + (q_1^{z_1} \ldots q_s^{z_s})^2 = 2y^n,$$

in non-negative integers $x, y, z_1, \ldots, z_s, n$, with $n \geq 3$ odd and $\gcd(x, y) = 1$, we have $n \ll sP^2 \log P$. Compare with Exercise 3.6.

EXERCISE 6.9. Let α_1 and α_2 be positive real numbers. Let p be a prime number. Let x_1 and x_2 be positive integers with $|x_i|_p^{-1} \ge x_i^{\alpha_i}$ for $i = 1, 2$. Prove that, for every odd prime number q which is coprime to $p - 1$ and every non-negative integers a, b, y such that

$$x_1^a + x_2^b + 1 = y^q,$$

we have $q \ll (\alpha_1 \alpha_2)^{-1}$.

EXERCISE 6.10. Assume that there exist integers a, b, y, q and a non-zero rational number t such that $a > b > 0$, $y \ge 2$, $q \ge 2$, and

$$2^a + 2^b + 1 = ty^q.$$

Prove that $q \ll \max\{1, h(t)\}$.

EXERCISE 6.11 (see [117]). Prove the p-adic analogues of Theorems 3.6 and 5.2, that is, establish effective irrationality measures for p-adic n-th roots of rational numbers.

EXERCISE 6.12 (see [103, 126]). Let p be a prime number and a, b positive integers not divisible by p. Let x, y, m, n be integers such that $n \ge 2$, $\gcd(x, y) = 1$, and $p^m = ax^n + by^n$. Prove that $n \ll p(\log p)(\log \max\{a, b, 2\})$. Discuss the extension of this result to the equation $q_1^{u_1} \cdots q_s^{u_s} = ax^n + by^n$, where $q_1, \ldots, q_s$ are given prime numbers and $u_1, \ldots, u_s$ are non-negative unknown integers.

EXERCISE 6.13. Establish that

$$P[x^m \pm 2^n] \gg \log m \, \frac{\log \log m}{\log \log \log m}$$

holds for any odd integer x and any integer m with $m \ge 16$.

6.12. Notes

▷ Brumer [99] used his p-adic analogue of Baker's theorem [16] to establish, following Ax [14], that the p-adic regulator of any abelian extension of the field of rationals (or of an imaginary quadratic field) does not vanish.

▷ Mahler [282] showed that (6.5) holds for every sufficiently large n, but his proof, based on Ridout's Theorem A.8, is ineffective in the sense that it does not yield an explicit value n_0 with the property that (6.5) holds for every n greater than n_0. Corvaja and Zannier [158] extended Mahler's result to lower bounds for $\|\alpha^n\|$, where α is a real algebraic number greater than 1 satisfying some necessary conditions. Their proof rests on the Schmidt subspace theorem and is thus not effective; see also [249]. It would be very interesting to have effective versions of these results.

▷ Corvaja and Zannier [159] managed to avoid the use of Theorem 2.13 in their proof that (6.15) has only finitely many solutions. They combined lower bounds for linear forms in two p-adic logarithms (say, Theorem 2.12) with the hypergeometric method of Thue and Siegel, based on Padé approximation to the binomial function. Actually, linear forms in p-adic logarithms close to 1 combine well with the hypergeometric method; see [52] and [109, 255, 350].

▷ Arithmetical properties of weighted sums of S-units have been studied in [215]. Lower bounds for the greatest prime factor of solutions to decomposable form equations are discussed in [178].

▷ For applications of S-unit equations, see e.g. the survey [184] and the recent monograph [182].

▷ Levesque and Waldschmidt [262] used the theory of linear forms in logarithms to construct parametric families of Thue–Mahler equations of arbitrary degree having only finitely many solutions; see also [117]. By means of a totally different method, Bennett and Dahmen [55] solved completely some specific families of Thue–Mahler equations of small degree and where the corresponding set of prime numbers is unbounded.

▷ In 1980, by using the theory of linear forms in complex and p-adic logarithms, Agrawal, Coates, Hunt, and van der Poorten [2] solved completely a cubic Thue–Mahler equation. This enables them to determine all elliptic curves defined over $\mathbb{Q}$ of conductor 11. The first general practical method for solving a Thue–Mahler equation was given by Tzanakis and de Weger [422] in 1992; see also [382].

▷ The resolution of S-unit equations, Thue–Mahler equations, and other classical Diophantine equations using modularity of Galois representation is discussed in [50, 55, 237, 240].

▷ Theorem 4.2 of Koymans [244] extends Theorem 6.13.

▷ A p-adic generalization of Theorem 4.11 has been worked out by van der Poorten [334]; see also Chapter 12 of [376], Chapter VII of [386], Brindza [93], and Koymans [244].

▷ Let p, q be distinct prime numbers and a, b, c, d non-zero integers. By a subtle combination of estimates for linear forms in complex and p-adic logarithms, Vojta [425] (see also [263]), Skinner [381], Mo and Tijdeman [304], and Mo [303], among other authors, have established effectively computable upper bounds for the solutions w, x, y, z in non-negative integers to the exponential equations $ap^x q^y + bp^z + cq^w + d = 0$ and $ap^x + bq^y + cp^z + dq^w = 0$.

▷ Let S be a finite set of places on an algebraic number field and assume that S contains the infinite places. Levin [263] applied the theory of linear forms in logarithms to deduce effective results for S-integral points on certain higher-dimensional varieties when the cardinality of S is sufficiently small. He generalized an effective result of Vojta [425] on the three-variable unit equation by giving an effective solution of the polynomial unit equation $f(u, v) = w$, where u, v, and w are S-units, the cardinality of S is at most 3, and f is a polynomial satisfying certain conditions, which are generically satisfied.

▷ Bugeaud and Kaneko [128] established, in a quantitative form, that any sufficiently large odd integer cannot have simultaneously only very small prime factors and few non-zero binary digits.

Chapter 7
Primitive divisors and the greatest prime factor of $2^n - 1$

This chapter is devoted to the study of primitive divisors in some special linear recurrence sequences of algebraic integers, with a special emphasis on Lucas and Lehmer sequences. Furthermore, we establish that the greatest prime factor of $2^n - 1$ tends to infinity faster than any linear function of n, thereby solving a conjecture formulated by Erdős [177] in 1965.

Throughout this chapter, we use several classical arithmetical functions, including the Möbius function μ and Euler's totient function φ. Their definitions and some of their basic properties are recalled in Appendix D. For every positive integer d, we denote by $\Phi_d(X, Y)$ the d-th homogeneous cyclotomic polynomial defined by

$$\Phi_d(X, Y) := \prod_{\zeta} (X - \zeta Y),$$

where the product is taken over all the primitive d-th roots of unity ζ. Observe that $\varphi(d)$ is the degree of $\Phi_d(X, Y)$.

7.1. Primitive divisors

We begin with the general definition of a primitive divisor.

Definition 7.1. Let K be an algebraic number field. Let $(a_n)_{n\geq 1}$ be a sequence of non-zero algebraic integers in K. Let $n \geq 2$ be an integer. A prime ideal $\mathfrak{p}$ of K is called a primitive divisor of a_n if $\mathfrak{p}$ divides the principal ideal generated by a_n, but does not divide any principal ideal generated by a_m, where $1 \leq m < n$.

The first general result about the existence of primitive divisors dates back to 1892, when Zsigmondy [452] proved that, if a and b are coprime non-zero integers with $|ab| \geq 2$, then $a^n - b^n$ has a primitive divisor for $n > 6$. The particular case $b = 1$ was done a few years earlier by Bang [39]. Zsigmondy's result is best possible, since $2^6 - 1 = (2^2 - 1)^2(2^3 - 1)$. It was rediscovered by Birkhoff and Vandiver [78] in 1904.

The next result has been established by Schinzel [355]; see also [393].

Theorem 7.2. *Let a and b be non-zero algebraic integers in an algebraic number field K such that $\frac{a}{b}$ is not a root of unity and the principal ideals generated by a and b in K are coprime. Then, there exists an effectively computable integer n_0, depending only on the degree of $\frac{a}{b}$, such that $a^n - b^n$ has a primitive divisor for every n greater than n_0.*

Proof. For simplicity, we content ourselves to prove the existence of an integer n_0 depending on the degree d of K and with the property stated in the theorem. A similar result where n_0 depends on a and b was established earlier in [338]. Without any loss of generality, we assume that $|a| \geq |b|$. Let $m \geq 2$ be an integer. If $|a| > |b|$, then

$$|a^m - b^m| \geq |a^m| \left|1 - \left(\frac{b}{a}\right)^m\right| \geq |a^m| \left(1 - \left|\frac{b}{a}\right|^2\right).$$

Since

$$\log\left(1 - \left|\frac{b}{a}\right|^2\right) \geq -dh\left(1 - \left|\frac{b}{a}\right|^2\right) \geq -2dh\left(\left|\frac{b}{a}\right|\right) - d\log 2 \gg -d^4 h\left(\frac{a}{b}\right),$$

by Theorems B.5, B.8, and 10.1, we derive that

$$\log|a^m - b^m| - m\log|a| \gg -d^4 h\left(\frac{a}{b}\right).$$

If $|a| = |b|$, then $\frac{a}{b}$ is a complex number on the unit circle and we deduce from Theorems 2.6 and 10.1 that

$$\log\left|\left(\frac{b}{a}\right)^m - 1\right| \gg -d^5 h\left(\frac{a}{b}\right)(\log m)^2.$$

Thus, in both cases, we get

$$\log|a^m - b^m| - m\log|a| \gg -d^5 h\left(\frac{a}{b}\right)(\log m)^2. \tag{7.1}$$

Let $n \geq 2$ be an integer. By the Möbius inversion formula, we have

$$\Phi_n(X,Y) = \prod_{m|n} (X^m - Y^m)^{\mu(n/m)}, \tag{7.2}$$

where μ denotes the Möbius function. We will estimate from below and from above the absolute value of the norm of $\Phi_n(a,b)$.

Let $\omega(n)$ denote the number of distinct prime factors of n. For any infinite place v of K, set $d_v = 1$ if v is real and $d_v = 2$ otherwise. By (7.1) applied with a and b replaced by their Galois conjugates, there exists an effectively computable absolute real number c such that

$$\begin{aligned}\log|\operatorname{Norm}_{K/\mathbb{Q}} \Phi_n(a,b)| &= \sum_{v\in M_K^\infty} \sum_{m|n} \mu\left(\frac{n}{m}\right) \log|a^m - b^m|_v^{d_v} \\ &\geq \left(\sum_{v\in M_K^\infty} \sum_{m|n} \mu\left(\frac{n}{m}\right) \left(m \log\max\left\{|a|_v^{d_v}, |b|_v^{d_v}\right\}\right)\right) \\ &\qquad\qquad - c d^6 h\left(\frac{a}{b}\right) \sum_{\substack{m|n,\\ \mu(n/m)\neq 0}} (\log m)^2 \\ &\geq \varphi(n)\, h\left(\frac{a}{b}\right) - c d^6 h\left(\frac{a}{b}\right) 2^{\omega(n)} (\log n)^2,\end{aligned}$$

since $|\mathrm{Norm}_{K/\mathbb{Q}}\, b| \geq 1$ and $\sum_{m|n} \mu(\frac{n}{m})m = \varphi(n)$, by Theorem D.6. As $\frac{a}{b}$ is not a root of unity, its height is positive, by Theorem B.6. It then follows from Theorem 10.1 and Theorems D.4 and D.5, on the behaviour of the functions φ and ω, that there exists an effectively computable positive integer $n_0(d)$, depending only on d, such that

$$|\mathrm{Norm}_{K/\mathbb{Q}}\, \Phi_n(a,b)| \geq \mathrm{e}^{\sqrt{n}}, \quad \text{for } n > n_0(d). \tag{7.3}$$

Let $\mathfrak{p}$ be a prime ideal of K. By Lemma 7.3 below, if $n \geq 4^d$ and $\mathfrak{p}$ is not a primitive divisor of $a^n - b^n$, then $\mathrm{v}_p(\Phi_n(a,b)) \leq \mathrm{v}_p(n)$, where p is the prime number lying below $\mathfrak{p}$. Consequently, if the ideal generated by $a^n - b^n$ has no primitive divisor and $n \geq 4^d$, then

$$|\mathrm{Norm}_{K/\mathbb{Q}}\, \Phi_n(a,b)| \leq n^d. \tag{7.4}$$

Let n be an integer exceeding $n_0(d)$ and 4^d. It then follows from (7.3) that (7.4) cannot hold, hence, the ideal generated by $a^n - b^n$ must have a primitive divisor. This proves the theorem. □

Lemma 7.3. *Let a and b be non-zero algebraic integers in a number field K of degree d such that $\frac{a}{b}$ is not a root of unity and the principal ideals generated by a and b in K are coprime. Let n be a positive integer and $\mathfrak{p}$ a prime ideal in K such that $\mathfrak{p}$ divides $\Phi_n(a,b)$ but $\mathfrak{p}$ is not a primitive divisor of $a^n - b^n$. If $n \geq 4^d$, then we have*

$$\mathrm{v}_p(\Phi_n(a,b)) \leq \mathrm{v}_p(n),$$

where p is the prime number lying below $\mathfrak{p}$.

Proof. We follow Postnikova and Schinzel [338]; see also [355]. For $i \geq 1$, let λ_i denote the smallest positive λ such that $\mathfrak{p}^i$ divides $a^\lambda - b^\lambda$. Let e be the ramification index of $\mathfrak{p}$ (see Section B.1) and set $k := \lfloor \frac{e}{p-1} \rfloor$. For a non-zero algebraic number α in K, let $\mathrm{v}_\mathfrak{p}(\alpha)$ denote the exponent of $\mathfrak{p}$ in the decomposition of the fractional ideal αO_K in a product of prime ideals, and recall that $\mathrm{v}_p(\alpha) = \frac{\mathrm{v}_\mathfrak{p}(\alpha)}{e}$. Let m be a positive integer. If m is not a multiple of λ_1, then $\mathrm{v}_\mathfrak{p}(a^m - b^m) = 0$. If m is a multiple of λ_1, but not of λ_2, then $\mathrm{v}_\mathfrak{p}(a^m - b^m) = 1$. And so on. If m is a multiple of λ_k, but not of λ_{k+1}, then $\mathrm{v}_\mathfrak{p}(a^m - b^m) = k$. Furthermore, if m is a multiple of λ_{k+1}, then, using the binomial theorem as in the proof of Lemma F.2, we get

$$\mathrm{v}_\mathfrak{p}(a^m - b^m) = \mathrm{v}_\mathfrak{p}(a^{\lambda_{k+1}} - b^{\lambda_{k+1}}) + \mathrm{v}_\mathfrak{p}\Big(\frac{m}{\lambda_{k+1}}\Big),$$

since $k + 1 > \frac{e}{p-1}$. Consequently, we obtain

$$\begin{aligned} \mathrm{v}_\mathfrak{p}(\Phi_n(a,b)) &= \sum_{m|n} \mu\Big(\frac{n}{m}\Big)\, \mathrm{v}_\mathfrak{p}(a^m - b^m) \\ &= \sum_{i=1}^{k} \sum_{\substack{m|n \\ \lambda_i|m}} \mu\Big(\frac{n}{m}\Big) + \sum_{\substack{m|n \\ \lambda_{k+1}|m}} \mu\Big(\frac{n}{m}\Big)\, (\mathrm{v}_\mathfrak{p}(a^{\lambda_{k+1}} - b^{\lambda_{k+1}}) - k) \\ &\qquad\qquad + \sum_{\substack{m|n \\ \lambda_{k+1}|m}} \mu\Big(\frac{n}{m}\Big)\, \mathrm{v}_\mathfrak{p}\Big(\frac{m}{\lambda_{k+1}}\Big). \end{aligned} \tag{7.5}$$

If $k = 0$, then we get $\lambda_1 < n$ since $\mathfrak{p}$ divides the ideal generated by $a^n - b^n$ but is not a primitive divisor of $a^n - b^n$. If $k \geq 1$, then $p \leq e + 1$ and, as $\mathfrak{p}^{k+1}$ divides the ideal generated by $a^\ell - b^\ell$, where ℓ denotes the cardinality of the group of invertible elements of $O_K/\mathfrak{p}^{k+1}$, we have

$$\lambda_{k+1} \leq \mathrm{Norm}_{K/\mathbb{Q}}\ \mathfrak{p}^k \times \big(\mathrm{Norm}_{K/\mathbb{Q}}\ \mathfrak{p} - 1\big).$$

Since the norm of $\mathfrak{p}$ over $\mathbb{Q}$ is at most equal to $p^{d/e}$, we obtain

$$\lambda_{k+1} \leq p^{kd/e}((e+1)^{d/e} - 1) \leq p^{d/(p-1)}(2^d - 1) < 4^d \leq n.$$

From the inequalities $\lambda_1 \leq \cdots \leq \lambda_{k+1} < n$, we get by Theorem D.6 that

$$\sum_{\substack{m \mid n \\ \lambda_i \mid m}} \mu\Big(\frac{n}{m}\Big) = 0, \quad i = 1, \ldots, k+1. \tag{7.6}$$

By plugging (7.6) into (7.5), we obtain

$$\mathrm{v}_\mathfrak{p}(\Phi_n(a,b)) = \sum_{\ell \mid (n/\lambda_{k+1})} \mu(\ell)\, \mathrm{v}_\mathfrak{p}\Big(\frac{n/\lambda_{k+1}}{\ell}\Big).$$

This last sum is smaller than its term corresponding to $\ell = 1$, giving

$$\mathrm{v}_\mathfrak{p}(\Phi_n(a,b)) \leq \mathrm{v}_\mathfrak{p}\Big(\frac{n}{\lambda_{k+1}}\Big) \leq \mathrm{v}_\mathfrak{p}(n).$$

This proves the lemma. □

7.2. Primitive divisors of Lucas–Lehmer sequences

Theorem 7.2 addresses arbitrary sequences of the form $(a^n - b^n)_{n\geq 1}$, where a and b are non-zero algebraic integers. In this section, we focus on two families of integer sequences of a similar type, the Lucas and Lehmer sequences. Their primitive divisors have been extensively studied since more than one century.

A *Lucas pair* is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. Given a Lucas pair (α, β), the corresponding sequence of *Lucas numbers* (or *Lucas sequence*, not to be confused with the sequence $(L_n)_{n\geq 0}$ defined in Section 3.7) is defined by

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n \geq 0.$$

A *Lehmer pair* is a pair (α, β) of algebraic integers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. For a Lehmer pair (α, β), the corresponding sequence of *Lehmer numbers* (or *Lehmer sequence*) is defined by

$$\widetilde{u}_n = \widetilde{u}_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \text{if } n \geq 1 \text{ is odd},$$

$$\widetilde{u}_n = \widetilde{u}_n(\alpha,\beta) = \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, \quad \text{if } n \geq 0 \text{ is even.}$$

Notice that every Lucas pair (α, β) is also a Lehmer pair, and

$$\begin{aligned} u_n &= \widetilde{u}_n, && \text{if } n \geq 1 \text{ is odd,} \\ u_n &= (\alpha+\beta)\widetilde{u}_n, && \text{if } n \geq 0 \text{ is even.} \end{aligned}$$

Let (α, β) be a Lehmer pair and $n \geq 2$ an integer. A prime number p is a *primitive divisor* of $\widetilde{u}_n(\alpha,\beta)$ if p divides $\widetilde{u}_n$ but does not divide $(\alpha^2-\beta^2)^2\widetilde{u}_1\cdots\widetilde{u}_{n-1}$. This provides a proper ("not merely automatical", as written by Schinzel [353]) generalization of the notion of primitive divisors introduced in Definition 7.1.

Similarly, let (α, β) be a Lucas pair and $n \geq 2$ an integer. A prime number p is a *primitive divisor* of $u_n(\alpha,\beta)$ if p divides u_n but does not divide $(\alpha-\beta)^2u_1\cdots u_{n-1}$. To illustrate this notion, we observe that, among the first Fibonacci numbers

$$\underline{1}, \underline{1}, 2, 3, \underline{5}, \underline{8}, 13, 21, 34, 55, 89, \underline{144}, 233, 377, 610, 987, 1597, \ldots$$

the underlined ones have no primitive divisors. Actually, these are all the Fibonacci numbers without a primitive divisor, as was proved by Carmichael [142] in 1913.

The following problem goes back to the beginning of the twentieth century, though it does not seem to have been ever formulated explicitly.

Problem 7.4. *List all Lucas and Lehmer numbers without primitive divisors. Classify all the triples* (α, β, n) *such that* (α, β) *is a Lucas (resp.,Lehmer) pair and* $u_n(\alpha,\beta)$ *(resp.,* $\widetilde{u}_n(\alpha,\beta)$*) has no primitive divisors.*

Throughout the end of this section, it is convenient to use the following terminology. A Lucas (*resp.,* Lehmer) pair (α, β) such that $u_n(\alpha,\beta)$ (*resp.,* $\widetilde{u}_n(\alpha,\beta)$) has no primitive divisors is called an n*-defective* Lucas (*resp.,* Lehmer) pair. Note that for any integer $n \geq 3$, a Lucas pair is an n-defective Lucas pair if and only if it is an n-defective Lehmer pair.

The very first results towards the resolution of Problem 7.4 have been listed below Definition 7.1. In 1913 Carmichael [142] proved that if (α, β) is a Lucas pair composed of real numbers, then $u_n(\alpha,\beta)$ has a primitive divisor for $n > 12$. Since the 12-th Fibonacci number, namely 144, has no primitive divisors, this is best possible. Carmichael's result was extended by Ward [436] (see [393, Lemma 8]) to Lehmer pairs (α, β) such that α^2 and β^2 are real numbers; see also Durst [174, 175].

The situation is much more complicated for the remaining Lucas and Lehmer pairs. "Nothing appears to be known about the intrinsic divisors of Lucas and Lehmer numbers when α and β are complex,"— wrote Ward [436, p. 230] in 1955. In 1962 Schinzel [352] completed the proof of the non-existence of n-defective Lucas and Lehmer pairs for n exceeding an effectively computable absolute integer n_0. While Carmichael and Ward used skillful but, in principle, elementary arguments, Schinzel's proof relies upon the theory of linear forms in (two) complex logarithms; see the proof of Theorem 7.2.

The next statement reproduces a result of Stewart [393], making explicit Schinzel's statement.

Theorem 7.5. *For* $n > \mathrm{e}^{452}2^{67}$*, there are no* n*-defective Lucas pairs. For* $n > \mathrm{e}^{452}4^{67}$*, there are no* n*-defective Lehmer pairs.*

Since there are infinitely many Lucas and Lehmer pairs, this result is not sufficient to reduce the complete determination of all n-defective Lucas–Lehmer pairs to a finite amount of computation. To do this, one needs an additional argument, which has been given by Stewart in [393].

Theorem 7.6. *For any integer n in $\{7, 9, 11\}$ or satisfying $n \geq 13$, there are only finitely many n-defective Lucas and Lehmer pairs.*

The condition on n is best possible, since, as proved in [393], for any integer n in $\{1, 2, 3, 4, 5, 6, 8, 10, 12\}$, there exist infinitely many n-defective Lehmer pairs.

We gather in a lemma several useful auxiliary results established in [392] and whose (elementary, but not easy) proofs are left to the reader. Recall that $P[\cdot]$ denotes the greatest prime factor.

Lemma 7.7. *Let (α, β) be a Lehmer pair. If $n \geq 5$ and $n \neq 6, 12$, then $P[n/\gcd(3, n)]$ divides $\Phi_n(\alpha, \beta)$ to at most the first power. All other prime factors of $\Phi_n(\alpha, \beta)$ are congruent to 1 or -1 modulo n. For n in $\{7, 9, 11\}$ or $n \geq 13$ the algebraic integers $\widetilde{u}_n$ and u_n have a primitive divisor whenever $\Phi_n(\alpha, \beta)$ is different from ± 1 and $\pm P[n/\gcd(3, n)]$.*

Proof of Theorem 7.6. The key point is to reduce the problem to a family of Thue equations. Let (α, β) be a Lehmer pair. Let denote by $(\widetilde{u}_n)_{n\geq 0}$ the corresponding Lehmer sequence and, if $\alpha + \beta$ is an integer, by $(u_n)_{n\geq 0}$ the corresponding Lucas sequence. Let $n \geq 7$ be an integer. Since

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta),$$

any primitive divisor of $\widetilde{u}_n$ or u_n also divides $\Phi_n(\alpha, \beta)$. Assume that n does not belong to $\{8, 10, 12\}$ and, in view of Theorem 7.5, that $n \leq e^{452} 4^{67}$.

Set $\zeta := e^{2i\pi/n}$. Let k be the largest integer smaller than $\frac{n}{2}$ and such that k and n are coprime. Then,

$$\begin{aligned}\Phi_n(\alpha, \beta) &= \prod_{\substack{1\leq j\leq k,\\ \gcd(j,n)=1}} (\alpha - \zeta^j \beta)(\alpha - \zeta^{-j} \beta)\\ &= \prod_{\substack{1\leq j\leq k,\\ \gcd(j,n)=1}} (\alpha^2 + \beta^2 - (\zeta^j + \zeta^{-j})\alpha\beta).\end{aligned}$$

Observe that $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$ is an integer. Put $\alpha^2 + \beta^2 = v$ and $\alpha\beta = w$. Define the homogeneous binary form $f_n(X, Y)$ by

$$\Phi_n(\alpha, \beta) = f_n(v, w) = \prod_{\substack{1\leq j\leq k,\\ \gcd(j,n)=1}} (v - (\zeta^j + \zeta^{-j})w).$$

The polynomial $f_n(X, 1)$ has degree $\varphi(n)/2$ and distinct roots. Our assumption on n implies that $\varphi(n) \geq 6$, thus the degree of the homogeneous binary form $f_n(X, Y)$ is greater than or equal to 3. By Theorem 4.5, the Thue equation

$$f_n(v, w) = a,$$

where a is in $\{\pm 1, \pm P[n/\gcd(3,n)]\}$, has only finitely many solutions. Each solution (v, w) to this equation gives rise to two solutions (α, β) and $(-\alpha, -\beta)$ to the equation

$$\Phi_n(\alpha, \beta) = a. \tag{7.7}$$

We then deduce from Lemma 7.7 that we can effectively find all the solutions to the equations (7.7) and establish the finite list of all Lucas–Lehmer pairs (α, β) whose n-th term has no primitive divisor, for some integer $n \geq 7$ with $n \notin \{8, 10, 12\}$. □

The lower bound in Theorem 7.5 was reduced to 30030 by Voutier [427,428]. In view of Theorem 7.6 and its proof, solving Problem 7.4 reduces to the resolution of finitely many Thue equations of degree less than 30030. This programm was successfully carried out by Bilu, Hanrot, and Voutier [77].

Theorem 7.8. *For every integer n greater than* 30*, the n-th term of any Lucas or Lehmer sequence has a primitive divisor.*

The proof of Theorem 7.8 required the complete resolution of several Thue equations of very large degree [74].

Furthermore, the authors of [77] also listed for every $n \leq 30$ all Lucas and Lehmer sequences whose n-th term has no primitive divisors. Four lists were composed: n-defective Lucas sequences for $n \leq 30$ and $\varphi(n) > 2$, as well as n-defective Lehmer sequences for $n \leq 30$ and $\varphi(n) > 4$, were listed by Voutier [426], while n-defective Lucas sequences for $n = 1, 2, 3, 4, 6$ and n-defective Lehmer sequences for $n = 1, \ldots, 6, 8, 10, 12$ were listed in [77]. There are several omissions in these lists and the reader is referred to [1] for the complete list of n-defective Lucas sequences for $n = 1, 2, 3, 4, 6$ and n-defective Lehmer sequences for $n = 1, \ldots, 6, 8, 10, 12$.

Theorem 7.8 has many important applications to Diophantine equations.

7.3. The Diophantine equation $x^2 + C = y^n$, continued

The equation $x^2 + C = y^n$ was already discussed in Section 4.6. We content ourselves to explain how its resolution is deeply connected to Theorem 7.8.

We focus on the case $C = 2$ and let x, y, q be positive integers with q an odd prime such that

$$x^2 + 2 = y^q.$$

Arguing as in the proof of Theorem 4.8, there exist rational integers a, b such that

$$x + \mathrm{i}\sqrt{2} = (a + \mathrm{i}b\sqrt{2})^q.$$

By equating the imaginary parts of both members of the previous equality, we deduce that $b = \pm 1$, thus

$$\left| \frac{(a + \mathrm{i}b\sqrt{2})^q - (a - \mathrm{i}b\sqrt{2})^q}{(a + \mathrm{i}b\sqrt{2}) - (a - \mathrm{i}b\sqrt{2})} \right| = \left| \frac{2\mathrm{i}\sqrt{2}}{2\mathrm{i}\sqrt{2}} \right| = 1.$$

This implies that the q-th term of the Lucas sequence defined by

$$u_n = \frac{(a + \mathrm{i}\sqrt{2})^n - (a - \mathrm{i}\sqrt{2})^n}{(a + \mathrm{i}\sqrt{2}) - (a - \mathrm{i}\sqrt{2})}, \quad n \geq 0,$$

has no primitive divisor and it follows from Theorem 7.8 that $q \leq 29$.

Clearly, some assumptions on C are required to apply Theorem 7.8 to the equation $x^2 + C = y^q$; see [138, 155] for precise statements.

7.4. On the number of solutions to the Diophantine equation $x^2 + D = p^n$

We have already mentioned the famous Ramanujan–Nagell equation $x^2 + 7 = 2^n$ in Section 4.6. In this section, we briefly discuss some closely related equations. We begin by a result of Beukers [64], who improved an earlier work by Apéry [12].

Theorem 7.9. *Let D be an odd, positive integer. Then, the equation*

$$x^2 + D = 2^n$$

has at most one solution in positive integers x and n, unless $D = 7$, 23 or $2^m - 1$ for some $m \geq 4$. The solutions in these exceptional cases are given by

$$\begin{aligned} &D = 7, && (x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15); \\ &D = 23, && (x, n) = (3, 5), (45, 11); \\ &D = 2^m - 1\ (m \geq 4), && (x, n) = (1, m), (2^{m-1} - 1, 2m - 2). \end{aligned}$$

While the proof of Theorem 7.9 does not rest on the theory of linear forms in logarithms, Theorem 7.8 is a crucial ingredient in the proof of Theorem 7.10 below, established by Bugeaud and Shorey [139]. It improves an earlier work by Apéry [13] and complements Theorem 7.9.

Theorem 7.10. *Let D be a positive integer and p an odd prime, not dividing D. Then, the Diophantine equation*

$$x^2 + D = p^n \tag{7.8}$$

has at most one solution in positive integers x and n, unless $(p, D) = (3, 2)$ or $(p, D) = (4a^2 + 1, 3a^2 + 1)$ for some positive integer a. In these exceptional cases, there are precisely two such solutions.

If we remove the coprimeness assumption $\gcd(p, D) = 1$ in Theorem 7.10, then the exceptional pairs are given by $(p, D) = (3, 2 \times 3^{2j})$ or $(p, D) = (4a^2 + 1, (3a^2 + 1)(4a^2 + 1)^{2j})$ for some positive integer a and some non-negative integer j; see Theorem 12.1 of [42].

Theorems 7.9 and 7.10 show that the Ramanujan–Nagell equation $x^2 + 7 = 2^n$ is exceptional, in the sense that it has *much more* solutions than the other equations of similar type.

As already noted by Beukers [63] (see also [139]), distinct solutions in positive integers x and n to (7.8) correspond to integers $\ell \geq 2$ for which

$$u_\ell := \frac{\lambda^\ell - (\lambda^\sigma)^\ell}{\lambda - \lambda^\sigma} = \pm 1, \tag{7.9}$$

where λ is an algebraic integer in $\mathbb{Q}(\sqrt{-D})$ and λ^σ denotes its Galois conjugate. Here, u_ℓ is the ℓ-th term of a Lucas or Lehmer sequence. The key tool for the proof of Theorem 7.10

(and for the results from [139]) is Theorem 7.8, which applies to (7.9). It is interesting to note that this result, which depends ultimately on estimates for linear forms in logarithms, is used to get a quantitative result, namely an upper bound for a number of solutions.

Actually, a more general result has been obtained in [139] (see also [259]) on equations of the form

$$D_1x^2 + D_2 = bk^n, \quad \text{in integer unknowns } x \geq 1, n \geq 1, \tag{7.10}$$

when D_1 and D_2 are positive integers, the positive integer k is coprime with the product D_1D_2, and b is in $\{1, 2, 4\}$, such that $b = 4$ when k is even. Then, Equation (7.10) has at most one solution, except in some cases, which are explicitly listed (and the exact number of solutions in these cases is known).

7.5. On the greatest prime factor of $2^n - 1$

Let $n \geq 7$ be an integer and p a primitive divisor of $2^n - 1$. Then, the order of 2 modulo p is equal to n. Since this order divides $p - 1$, we deduce that p is congruent to 1 modulo n and, consequently, that $P[2^n - 1]$ is at least equal to $n + 1$. In 1965 Erdős [177] conjectured that

$$\lim_{n\to+\infty} \frac{P[2^n - 1]}{n} = +\infty.$$

In this section, we combine an estimate of Yamada [442] on linear forms in two p-adic logarithms with an approach of Stewart [400] to prove Erdős' conjecture.

Specifically, we establish the following result.

Theorem 7.11. *Let a, b be integers with $a > b \geq 1$. For any integer $n \geq 3$, the greatest prime factor of $a^n - b^n$ satisfies*

$$P[a^n - b^n] \gg_b n\sqrt{\frac{\log n}{\log\log n}}.$$

This solves the above mentioned conjecture of Erdős. Actually, a stronger and more general result was proved in 2013 by Stewart [400]; see Theorem 7.13 below.

Birkhoff and Vandiver [78] attributed to Euler the first assertion of Lemma 7.12, but gave no precise reference. It extends the observation on $P[2^n - 1]$ made at the beginning of this section.

Lemma 7.12. *Let a, b be coprime integers with $a > b \geq 1$. For $n \geq 2$, every primitive prime divisor of $a^n - b^n$ is congruent to 1 modulo n. For any odd prime number p not dividing ab and any positive integer n we have*

$$\mathrm{v}_p(a^n - b^n) \leq \mathrm{v}_p(a^{p-1} - b^{p-1}) + \mathrm{v}_p(n). \tag{7.11}$$

Proof. We follow the argument of Stewart given in Section 6 of [400]. For simplicity, write $z_n = a^n - b^n$ for every positive integer n. Let p be an odd prime number not dividing ab. Let $\ell = \ell(p)$ be the smallest positive integer h for which p divides z_h. It is equal to the order of $\frac{a}{b}$ modulo p, hence ℓ divides $p - 1$ and ℓ divides every positive integer n such that p divides z_n. This implies that, for $n \geq 2$, every primitive divisor of z_n is congruent to 1 modulo n.

Let n be a positive integer such that p divides z_n. Assume that p divides $\Phi_n(a,b)$. Write $n = \ell t p^k$, where k is a non-negative integer and t is a positive integer not divisible by p. Observe that p divides $z_{n/t}$ since ℓ divides n/t. If $t > 1$, then $\Phi_n(a,b)$ divides $z_n/z_{n/t}$ and we get a contradiction by using Exercise 7.1. We conclude that $t = 1$ and $n = \ell p^k$. Since p is odd and, for any positive integer m, we have

$$\frac{z_{mp}}{z_m} = \frac{(z_m + b^m)^p - b^{mp}}{z_m} = pb^{m(p-1)} + \binom{p}{2} b^{m(p-2)} z_m + \cdots + z_m^{p-1},$$

we deduce that $\mathrm{v}_p(z_{mp}) = \mathrm{v}_p(z_m) + 1$ if p divides z_m. We have proved that

$$\mathrm{v}_p\big(\Phi_{\ell p^k}(a,b)\big) = 1, \qquad \text{for } k \geq 1,$$

and

$$\mathrm{v}_p\big(\Phi_m(a,b)\big) = 0, \qquad \text{if } m \text{ is not of the form } \ell p^k \text{ for } k \geq 0.$$

Let n be a positive integer. Since $z_n = \prod_{d \mid n} \Phi_d(a,b)$, this implies that

$$\mathrm{v}_p(z_n) = \mathrm{v}_p(z_\ell) + \mathrm{v}_p\Big(\frac{n}{\ell}\Big), \quad \text{if } \ell \text{ divides } n,$$

while we have $\mathrm{v}_p(z_n) = 0$ if ℓ does not divide n. As ℓ divides $p-1$, we derive that z_ℓ divides z_{p-1} and $\mathrm{v}_p(z_\ell) \leq \mathrm{v}_p(z_{p-1})$. Recalling that $\mathrm{v}_p(\ell) = 0$, we get the desired result. □

Proof of Theorem 7.11. We proceed as in the proof of Theorem 7.2, but the situation is much simpler since a and b are positive integers. For any positive integer m, we have

$$0 \geq \log(a^m - b^m) - m \log a = \log\Big(1 - \frac{b}{a}\Big)^m \geq \log\Big(\frac{a-b}{a}\Big) \geq -\log a.$$

Let $n > 12$ be an integer. It follows from (7.2) that

$$\Big|\log \Phi_n(a,b) - \sum_{m \mid n} m\mu\Big(\frac{n}{m}\Big) \log a\Big| \leq 2^{\omega(n)} \log a,$$

where $\omega(n)$ denotes the number of disctinct prime factors of n. By Theorems D.4, D.5, and D.6, we get

$$\log \Phi_n(a,b) \geq \varphi(n) \log a - 2^{\omega(n)} \log a \geq \frac{\varphi(n)}{2} \log a, \tag{7.12}$$

when n is sufficiently large. Let p be a prime number dividing $\Phi_n(a,b)$. Since a and b are coprime, p does not divide ab and

$$\mathrm{v}_p(\Phi_n(a,b)) \leq \mathrm{v}_p(a^n - b^n). \tag{7.13}$$

It then follows from Lemma 7.12 and Theorem 12.3 (note that we can as well apply Theorem 2.9) that

$$\begin{aligned} \mathrm{v}_p(a^n - b^n) &\le \mathrm{v}_p(a^{p-1} - b^{p-1}) + \mathrm{v}_p(n) \\ &\le 132 \cdot 10^5 \, \frac{p}{(\log p)^2} \, (\log 5a)\,(\log 5b) + \mathrm{v}_p(n). \end{aligned} \tag{7.14}$$

Let P_n denote the greatest prime factor of $\Phi_n(a,b)$. By Lemma 7.7 there is at most one prime factor of $\Phi_n(a,b)$ which is not congruent to ± 1 modulo n. This prime factor divides n and it divides $\Phi_n(a,b)$ to at most the first power. Bounding this prime factor by n, we get

$$\log \Phi_n(a,b) \le \log n + \sum_{p \le P_n,\, p \nmid n} (\log p)\, \mathrm{v}_p(\Phi_n(a,b)). \tag{7.15}$$

Combining (7.12), (7.14), and (7.15), we obtain

$$\varphi(n) \ll \log n + \sum_{\substack{p \le P_n, \\ p \equiv \pm 1 (n)}} \frac{p}{\log p} (\log 5b).$$

Using Theorem D.5 and Theorem D.7, which bounds from above the number of primes which are less than P_n and congruent to ± 1 modulo n, we obtain

$$\varphi(n) \ll_b \frac{P_n}{\varphi(n) \log(P_n/n)} \cdot \frac{P_n}{\log P_n} \ll_b \frac{P_n^2}{\varphi(n)(\log P_n)(\log(P_n/n))}.$$

It then follows from Theorem D.5 that there exists a positive real number C such that

$$P_n \gg_b n \sqrt{\log n} (\log \log n)^{-C}.$$

However, by using (D.3) instead of Theorem D.5, we derive the larger lower bound

$$P_n \gg_b n \sqrt{\frac{\log n}{\log \log n}}.$$

which proves the theorem, since $P[a^n - b^n] \ge P_n$, by (7.13). □

Stewart [400] established the following stronger and more general result.

Theorem 7.13. *If $(u_n)_{n \ge 0}$ is a Lucas or Lehmer sequence, then there exists an effectively computable integer n_0 such that, for any integer n greater than n_0, we have*

$$P[u_n] > n \, \exp\Big(\frac{\log n}{104 \log \log n}\Big).$$

The case of Lucas and Lehmer sequences with *irrational* roots is much more delicate than the special case considered in Theorem 7.11, since we have to deal with linear forms in logarithms of algebraic numbers lying in a quadratic number field. The dependence on p in Theorems 2.9 and 2.12 is then of order p^2, thus, we cannot adapt the proof of Theorem 7.11. New ideas are needed: Stewart [400] inflated artificially the number of terms which occur in the p-adic linear form in logarithms and applied a refined estimate of Yu [450].

Similar ideas allowed Stewart [401] to establish the following theorem, which improves an earlier result of Yu and Hung [451] (see also [126]).

THEOREM 7.14. *Let $(u_n)_{n\ge 0}$ be a non-degenerate binary recurrence sequence of integers. Then, there exists an effectively computable integer n_0 such that, for any integer n greater than n_0, we have*

$$P[u_n] > \sqrt{n}\ \exp\Big(\frac{\log n}{104 \log\log n}\Big).$$

We display a consequence of Theorem 7.14 to arithmetic properties of the convergents of quadratic numbers.

COROLLARY 7.15. *Let ξ be a quadratic real number and let $(p_n/q_n)_{n\ge 0}$ denote the sequence of its convergents. Then, for every sufficiently large integer n, we have*

$$P[q_n] \gg_{\xi} \sqrt{\log q_n}\ \exp\Big(\frac{\log\log q_n}{104 \log\log\log q_n}\Big).$$

Proof. Write $\xi = [a_0; a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{s-1}, b_0, \ldots, b_{s-1}, \ldots]$. In the course of the proof of Theorem 1 in [258], it is established that there exists an integer t such that

$$q_{n+2s} - t q_{n+s} + (-1)^s q_n = 0,$$

for every $n \ge r$. Set $M := \max\{a_1, \ldots, a_{r-1}, b_1, \ldots, b_{s-1}\}$. Then, for $n \ge 1$, an easy induction shows that $q_n \le (M+2)^n$ and, thus, $n \ge (\log q_n)/(\log(M+2))$. Combined with Theorem 7.14, this proves the corollary. □

7.6. Exercises

EXERCISE 7.1 (see [392]). Let (α, β) be a Lehmer pair and d, m, n positive integers. Prove that if d divides n, then $\gcd(u_n/u_d, u_d)$ divides n/d. Prove that $\gcd(u_n, u_m) = u_{\gcd(n,m)}$.

EXERCISE 7.2. Let a, b be coprime integers with $a > b \ge 1$. For an integer $t \ge 1$, let Q_t denote the product of the t first prime numbers. Prove that we have

$$\log P[a^{Q_t} - b^{Q_t}] \ll \frac{Q_t}{\log\log Q_t} \log a.$$

7.7. Notes

▷ With a non-torsion rational point $P = (x(P), y(P))$ on an elliptic curve written $y^2 = x^3 + ax + b$ in minimal form we can associate an elliptic divisibility sequence $(B_n(P))_{n\ge 1}$ defined, by using the addition law on the curve, by $x(nP) = A_n(P)/B_n(P)^2$ (in lowest terms). Silverman [380] established the analogue of Zsigmondy's theorem, namely that, for any given elliptic divisibility sequence $(B_n)_{n\ge 1}$, there exists an integer n_0 such that B_n has a primitive divisor for every $n \ge n_0$.

$\triangleright$ The only perfect powers in the Fibonacci sequence are $0, 1, 8$, and 144; see Theorem 3.14, the paper [137] and the references therein. Perfect powers in other Lucas and Lehmer sequences have been studied in [131, 379].

$\triangleright$ Stiller [406] established that the Diophantine equation $x^2 + 119 = 15 \cdot 2^n$ has exactly six solutions in positive integers; see Ulas [423] for further examples of similar equations with many solutions.

$\triangleright$ Let a, b be coprime positive integers. Murty and Wong [309] established that, for every positive real number ε, there exist real numbers c_1 and c_2, depending only on a, b, ε, such that the greatest prime power divisor of $a^n - b^n$ exceeds $c_1 n^{2-\varepsilon}$ and, under the abc-conjecture (see Chapter 8), such that $P[a^n - b^n]$ exceeds $c_2 n^{2-\varepsilon}$.

$\triangleright$ Let $(u_n)_{n\geq 0}$ be a Lucas or Lehmer sequence. Győry [213] established that, if $n > 30$ or if $6 < n \leq 30$ and $|u_n| > \exp\exp(7040)$, then $P[u_n] > \frac{1}{4}\sqrt{\log\log |u_n|}$.

Chapter 8
The abc-conjecture

In June 1985 Oesterlé [318] gave a lecture at the Max-Planck-Institute in Bonn. Motivated by conjectures about elliptic curves, he asked whether there is an absolute real number κ such that, for every positive, coprime integers a, b, we have

$$a + b \le \Bigl(\prod_{p \mid ab(a+b)} p \Bigr)^{\kappa},$$

where the product is taken over the distinct prime divisors of $ab(a + b)$. A few weeks thereafter, at a conference in London in honour of Roth's sixtieth birthday, Masser [285, 288] proposed the following refinement of the conjecture formulated by Oesterlé.

Conjecture 8.1 (abc-conjecture). *For every positive real number ε, there exists a positive real number $\kappa(\varepsilon)$, which depends only on ε, such that, for all positive integers a, b, and c with*

$$a + b = c \quad \textit{and} \quad \gcd(a, b, c) = 1, \tag{8.1}$$

we have

$$c < \kappa(\varepsilon) G^{1+\varepsilon}, \quad \textit{where } G = \prod_{p \mid abc} p. \tag{8.2}$$

In (8.2) and below, the product is taken over the distinct prime divisors of abc. The abc-conjecture is a very deep conjecture, with profound consequences; see Chapter 12 of [88] and the references given therein. We show in this chapter how the theory of linear forms in complex and p-adic logarithms applies to get a weaker version of (8.2).

8.1. Effective results towards the abc-conjecture

In 1986, applying an estimate for linear forms in p-adic logarithms of van der Poorten [335], Stewart and Tijdeman [402] established that, for all positive integers a, b, and c with (8.1), we have

$$\log c \ll \Bigl(\prod_{p \mid abc} p \Bigr)^{15}. \tag{8.3}$$

Subsequently, in 1991, Stewart and Yu [404] strengthened (8.3) by means of a subtle combination of estimates for complex and p-adic linear forms in logarithms. We state below the further improvement they obtained in 2001 in [405].

Theorem 8.2. *For all positive integers a, b, and c with $a + b = c$ and* $\gcd(a, b, c) = 1$, *we have*

$$\log c \ll G^{1/3}(\log G)^3, \quad \textit{where } G = \prod_{p \mid abc} p.$$

In the same paper [405], the authors derived another estimate in the direction of the abc-conjecture. Recall that $P[\cdot]$ denotes the greatest prime factor.

Theorem 8.3. *There exists an effectively computable real number κ such that, for all positive integers a, b, and c with $a + b = c$ and* $\gcd(a, b, c) = 1$, *we have*

$$\log c < p' G^{\kappa(\log\log\log(8G))/\log\log G},$$

where

$$G = \prod_{p \mid abc} p \quad \textit{and} \quad p' = \min\{P[a], P[b], P[c]\}.$$

We point out a consequence of Theorem 8.3, which should be compared with the lower bound for $P[f(x, y)]$ established in [217]; see also Sections 3.5 and 6.7.

Corollary 8.4. *For all positive integers a, b with $a < b$ and $b \geq 40$, we have*

$$P[ab(a + b)] \gg \log\log b \, \frac{\log\log\log b}{\log\log\log\log b}.$$

Proof. Set $P := P[ab(a + b)]$. Observe that

$$\log\Bigl(\prod_{p \mid ab(a+b)} p\Bigr) \leq \sum_{p \leq P} \log p \leq (\log P) \operatorname{Card}\{p \leq P : p \text{ prime}\} \ll P,$$

by Theorem D.2. It follows from Theorem 8.3 that there exists an effectively computable real number κ such that

$$\log\log b < \log P + \kappa \frac{P \log\log P}{\log P}.$$

This implies the corollary. □

8.2. Proofs of Theorems 8.2 and 8.3

Without any loss of generality, we suppose that $a < b$. To shorten the notation, write p_a, p_b, p_c instead of $P[a], P[b], P[c]$, respectively. Throughout this proof, $c_1, c_2, \ldots$ denote effectively computable positive numbers. Observe that $G \geq 6$ and put

$$G^* = \max\Bigl\{\frac{G}{p_a p_b p_c}, 16\Bigr\} \quad \text{and} \quad r = \omega(abc),$$

the number of distinct prime factors of abc.

Put $m = r - 2$ if $a = 1$ (in which case $p_a = 1$) and $m = r - 3$ otherwise. Observe that, by Theorem D.2,

$$\log G^* \geq \sum_{j=1}^{r-3} \log p_j \gg r \log r,$$

hence,

$$m \le r \ll \frac{\log G^*}{\log\log G^*}. \tag{8.4}$$

If $m \ge 1$, then the arithmetic-geometric mean inequality gives

$$\prod_{\substack{p|abc,\\ p\notin\{p_a,p_b,p_c\}}} \log p \le \Bigg(\frac{1}{m} \sum_{\substack{p|abc,\\ p\notin\{p_a,p_b,p_c\}}} \log p\Bigg)^m \le \Big(\frac{\log G^*}{m}\Big)^m.$$

We deduce that

$$\prod_{\substack{p|abc,\\ p\notin\{p_a,p_b,p_c\}}} \log p < \exp\Big(c_1 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big). \tag{8.5}$$

With the usual convention that the empty product is equal to 1, we see that (8.5) also holds if $m = 0$.

Let p be a prime divisor of abc. Our aim is to estimate $\mathrm{v}_p(abc)$. First, we assume that

$$p < \mathrm{e}^{(\log r)^2}. \tag{8.6}$$

Suppose that p divides c, the other two cases being analogous.

Then, p does not divide b and

$$\mathrm{v}_p(c) = \mathrm{v}_p\Big(\frac{c}{b}\Big) = \mathrm{v}_p\Big(\frac{a}{b}+1\Big) \le \mathrm{v}_p\Big(\Big(\frac{a}{b}\Big)^2 - 1\Big).$$

Write

$$\Big(\frac{a}{b}\Big)^2 - 1 = \prod_{j=1}^{\omega(ab)} q_j^{u_j} - 1,$$

for some non-zero integers u_j and distinct prime numbers $q_1, \dots, q_{\omega(ab)}$. Note that we have $|u_j| \le 3 \log c$ for $j = 1, \dots, \omega(ab)$.

It follows from Theorem 2.9 that

$$\mathrm{v}_p(c) \le p c_2^{\omega(ab)} \Big(\prod_{\ell|ab, \ell \text{ prime}} \log \ell\Big) \log\log c. \tag{8.7}$$

By (8.4), (8.5), and (8.6), this gives

$$\mathrm{v}_p(c) < \exp\Big(c_3 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big) (\log(2p_a)) (\log p_b) \log\log c. \tag{8.8}$$

The fact that, in Theorem 2.9, the dependence on the number n of algebraic numbers is exponential and not of the form n^{cn} is crucial here. Indeed, by using an earlier estimate we would have $c_2^{\omega(ab)}$ replaced by $\omega(ab)^{2\omega(ab)}$ in (8.7) and would then get an upper bound of the form

$$\mathrm{v}_p(c) < (G^*)^{c_4} (\log(2p_a)) (\log p_b) \log\log c,$$

which is much weaker than (8.8).

Similarly, we get

$$\mathrm{v}_p(b) < \exp\Big(c_5 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big)\,(\log(2p_a))\,(\log p_c)\,\log\log c \tag{8.9}$$

and

$$\mathrm{v}_p(a) < \exp\Big(c_6 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big)\,(\log p_b)\,(\log p_c)\,\log\log c. \tag{8.10}$$

We now define the quantities

$$R_a = \prod_{\ell \mid a, \ell \neq p_a}{}' \ell^{\mathrm{v}_\ell(a)}, \quad R_b = \prod_{\ell \mid b, \ell \neq p_b}{}' \ell^{\mathrm{v}_\ell(b)}, \quad R_c = \prod_{\ell \mid c, \ell \neq p_c}{}' \ell^{\mathrm{v}_\ell(c)},$$

where $\prod'$ means that ℓ runs through the prime numbers less than $\mathrm{e}^{(\log r)^2}$. Observe that

$$\begin{aligned} \log R_a &< \omega(a)\,(\log r)^2 \max_{\ell \mid a, \ell < \mathrm{e}^{(\log r)^2}} \mathrm{v}_\ell(a) \\ &\leq r(\log r)^2 \exp\Big(c_7 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big)\,(\log p_b)\,(\log p_c)\,\log\log c \\ &\leq \exp\Big(c_8 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big)\,(\log p_b)\,(\log p_c)\,\log\log c, \end{aligned}$$

by (8.10) and (8.4), and similarly for R_b and R_c.

Put $q_1 = -R_a/R_b$ and set

$$-\frac{a}{b} = q_1 q_2^{b_2} \cdots q_n^{b_n}, \tag{8.11}$$

where $b_2, \ldots, b_n$ are non-zero rational integers and $q_2, \ldots, q_n$ are distinct prime numbers exceeding $\mathrm{e}^{(\log r)^2}$ or in the set $\{p_a, p_b\}$. Observe that, by Theorem B.5, the height of q_1 satisfies

$$h(q_1) \leq \exp\Big(c_9 \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big)\,(\log\max\{p_a, p_b\})\,(\log p_c)\,\log\log c. \tag{8.12}$$

Using (8.11) to bound n, we get

$$(n-3)(\log r)^2 \leq \log G^*,$$

thus, if $r \geq (\log G^*)^{1/2}$, we obtain

$$n^{2n} < \exp\Big(c_{10} \frac{\log G^*}{\log\log G^*}\Big). \tag{8.13}$$

Since $n \leq r$, Inequality (8.13) also holds when $r < (\log G^*)^{1/2}$.

We are now in position to estimate $\mathrm{v}_p(abc)$ for an arbitrary prime factor p of abc. By (8.11), we have

$$\mathrm{v}_p(c) = \mathrm{v}_p(q_1 q_2^{b_2} \cdots q_n^{b_n} - 1).$$

Set

$$W_p = \exp\Big(c_{11} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big) \frac{p}{(\log p)^4} \times \Big(\prod_{\ell \in \{p_a, p_b, p_c\}} \log \max\{p, \ell\} \Big) (\log\log c)^2. \tag{8.14}$$

Using Theorem 2.10, it follows from a careful computation based on (8.4), (8.5), (8.12), and (8.13) that

$$\mathrm{v}_p(c) < W_p \log \max\{p_a, p_b\}. \tag{8.15}$$

The crucial point with the use of Theorem 2.10 here is that we do need a good dependence on the prime number p, while the weaker dependence on n does not cause any trouble in view of (8.13).

Similarly, we obtain

$$\mathrm{v}_p(b) < W_p \log \max\{p_a, p_c\}$$

and

$$\mathrm{v}_p(a) < W_p \log \max\{p_b, p_c\}.$$

These upper bounds for $\mathrm{v}_p(a)$, $\mathrm{v}_p(b)$, and $\mathrm{v}_p(c)$ are weaker than the upper bounds obtained in (8.8), (8.9), and (8.10), which are valid under the assumption (8.6). It would be much desirable to remove the factor p in (8.14).

Having estimated $\mathrm{v}_p(abc)$ for every prime divisor p of abc, we get

$$\log c = \sum_{p|c} \mathrm{v}_p(c) \log p \le r \max_{p|c} \{\mathrm{v}_p(c) \log p\}, \tag{8.16}$$

and similar upper bounds hold for $\log a$ and $\log b$. Set

$$L = \log \max\{p_a, p_b\} \cdot \log \max\{p_b, p_c\} \cdot \log \max\{p_a, p_c\}.$$

By (8.4), (8.14), (8.15), and (8.16), we then get

$$\frac{\log c}{(\log\log c)^2} < \exp\Big(c_{12} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big) \frac{p_c}{(\log p_c)^2} L. \tag{8.17}$$

Since $b > \frac{c}{2}$ and $c \ge 3$, we have

$$\log b > \log c - \log 2 > \frac{\log c}{4}, \tag{8.18}$$

thus

$$\log c < 4 \log b \le 4r \max_{p|b} \{\mathrm{v}_p(b) \log p\},$$

and, arguing as above, we deduce that

$$\frac{\log c}{(\log\log c)^2} < \exp\Big(c_{13} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Big) \frac{p_b}{(\log p_b)^2} L. \tag{8.19}$$

We distinguish two cases. First, assume that $a \geq \sqrt{b}$. Then, by (8.18),

$$\log a \geq \frac{\log b}{2} > \frac{\log c}{8}$$

and, similarly as above, we deduce from

$$\log c < 8 \log a \leq 8r \max_{p|a} \{\mathrm{v}_p(a) \log p\}$$

that

$$\frac{\log c}{(\log\log c)^2} < \exp\Bigl(c_{14} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Bigr) \frac{p_a}{(\log(2p_a))^2} L. \tag{8.20}$$

Second, assume that $a < \sqrt{b}$, in which case

$$\log\Bigl(\frac{a+b}{b}\Bigr) < \log\Bigl(1 + \frac{1}{\sqrt{b}}\Bigr) < \frac{1}{\sqrt{b}} < \sqrt{\frac{2}{c}}. \tag{8.21}$$

Put $q'_1 = R_c/R_b$ and write

$$\frac{c}{b} = q'_1 (q'_2)^{b'_2} \cdots (q'_n)^{b'_n},$$

where $b'_2, \ldots, b'_n$ are non-zero rational integers and $q'_2, \ldots, q'_n$ are distinct prime numbers exceeding $\mathrm{e}^{(\log r)^2}$ or in the set $\{p_b, p_c\}$. Then,

$$0 < \log\Bigl(\frac{a+b}{b}\Bigr) = \log\Bigl(\frac{c}{b}\Bigr) = \log q'_1 + b'_2 \log q'_2 + \cdots + b'_n \log q'_n.$$

By applying Theorem 2.2, we get

$$\log\log\Bigl(\frac{a+b}{b}\Bigr) > -\exp\Bigl(c_{15} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Bigr) \log\max\{p_b, p_c\} \\ \times (\log(2p_a)) (\log p_b) (\log p_c) (\log\log c)^2. \tag{8.22}$$

We deduce from (8.21) and (8.22) that

$$\frac{\log c}{(\log\log c)^2} < \exp\Bigl(c_{16} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Bigr) \log\max\{p_b, p_c\} \\ \times (\log(2p_a)) (\log p_b) (\log p_c).$$

Since

$$\log\max\{p_b, p_c\} (\log(2p_a)) (\log p_b) (\log p_c) \ll \frac{p_a}{(\log(2p_a))^2} L,$$

we see that (8.20) still holds when $a < \sqrt{b}$.

Let p', p'', and p''' be such that $p' < p'' < p'''$ and $\{p_a, p_b, p_c\} = \{p', p'', p'''\}$. It follows from (8.17), (8.19), and (8.20) that

$$\frac{\log c}{(\log\log c)^2} < \exp\Bigl(c_{17} \frac{\log G^* \log\log\log G^*}{\log\log G^*}\Bigr) \frac{p'}{(\log(2p'))^2} (\log p'') (\log p''')^2. \tag{8.23}$$

Proceeding as in the proof of (8.5) we get

$$(\log p'')\,(\log p''')^2 \leq \Bigl(\prod_{p|abc} \log p\Bigr)^2 < \exp\Bigl(c_{18}\frac{\log G \log\log\log \max\{G, 16\}}{\log\log G}\Bigr),$$

thus, by (8.23),

$$\frac{\log c}{(\log\log c)^2} < \exp\Bigl(c_{19}\frac{\log G \log\log\log \max\{G, 16\}}{\log\log G}\Bigr)\,\frac{p'}{(\log(2p'))^2}. \tag{8.24}$$

This proves Theorem 8.3.

To establish Theorem 8.2, we multiply (8.17), (8.19), and (8.20) together to get

$$\Bigl(\frac{\log c}{(\log\log c)^2}\Bigr)^3 < \exp\Bigl(c_{20}\frac{\log G^* \log\log\log G^*}{\log\log G^*}\Bigr) \\ \times \frac{p_a\,p_b\,p_c}{(\log(2p_a)\log p_b \log p_c)^2}\,(\log p'')^3\,(\log p''')^6. \tag{8.25}$$

We may assume that

$$p' > G^{1/4},$$

since otherwise Theorem 8.2 follows directly from (8.24). Then, we get from (8.25) that

$$\Bigl(\frac{\log c}{(\log\log c)^2}\Bigr)^3 \ll G^* p_a\,p_b\,p_c(\log G)^3 \ll G(\log G)^3,$$

and so

$$\log c \ll G^{1/3}(\log G)^3,$$

as asserted.

8.3. Exercise

Exercise 8.1. Let a, b, and c be positive integers as in (8.1) and define G as in (8.2). Let P be the greatest prime factor of abc. Let B denote the largest integer t such that p^t divides abc for some prime number p. Apply Theorem 2.9 with the prime number P to bound B from above in terms of G. Bound c from above in terms of B and G, and conclude that there exists an effectively computable real number κ such that

$$\log c < G \cdot G^{\kappa(\log\log\log(8G))/\log\log G}.$$

8.4. Notes

▷ Robert, Stewart, and Tenenbaum [348] have given very precise refinements of the abc-conjecture, which rest on the sole heuristic assumption that, if a and b are coprime, then the greatest squarefree factors of a, b, and $c = a + b$ are statistically independent.

▷ Keep the notation of Theorems 8.2 and 8.3. Using a different (and more direct) approach, also based on lower bounds for linear forms in complex and p-adic logarithms, Győry and Yu [217] have established that

$$\log c < 2^{23} \frac{P}{\log P} G^{653(\log\log\log \max\{G,16\})/(\log\log \max\{G,16\})}, \quad \text{where } P = P[abc].$$

Chi [146], following the proof of [405], has proved that

$$\log c < p' G^{13.6(\log\log\log \widetilde{G})/(\log\log G)}, \quad \text{where } \widetilde{G} = \max\{G, 9699690\}.$$

▷ By using the modularity of elliptic curves, Murty and Pasten [307] established that all positive integers a, b, c with $a + b = c$ satisfy

$$\log c \le 4.8G \log G + 13G + 25,$$

where G is as in (8.2); see also von Känel [236] for a slightly weaker result.

▷ Masser [286] extended the abc-conjecture to algebraic number fields; see also Browkin [98], Győry [214], and the references quoted therein.

▷ Let a, b, c be coprime positive integers satisfying $a + b = c$ (called an abc-triple in the sequel). Put $h = \log c$ and $r = r(a, b, c) = \sum_{p|abc} \log p$. The abc-conjecture asserts that for any positive ε there exists a real number $K(\varepsilon)$ such that $h \le r + \varepsilon h + K(\varepsilon)$. The choice $(a, b, c) = (1, 2^n, 2^n + 1)$ shows that there exists an infinite sequence of abc-triples such that $h \ge r - \log 2$. Stewart and Tijdeman [402] obtained a much sharper result: for any positive real number δ, there exist infinitely many abc-triples with $h \ge r + (4 - \delta)\sqrt{h}/\log h$. Van Frankenhuijsen [187] showed that, in the latter result, $4 - \delta$ can be replaced by 6.068.

▷ Baker [29–31] suggested modifications and strengthenings of the abc-conjecture which he related to earlier conjectures on lower bounds for linear forms in logarithms of algebraic numbers formulated in the Introduction to Chapters X and XI of [250]. An interesting connection is pointed out with conjectures on simultaneous complex and p-adic estimates for the same linear combination of logarithms; see also Philippon's papers [327,328]. Von Känel and Matschke [237] verified an explicit abc-conjecture of Baker ([30, Conjecture 4]) for all abc-triples with $\prod_{p|abc} p \le 10^7$.

▷ Additional information on and around the abc-conjecture can be found in the survey [283] and on the website maintained by Abderrahmane Nitaj `www.math.unicaen.fr/~nitaj/abc.html`.

Chapter 9

Simultaneous linear forms in logarithms and applications

A longstanding open problem in the theory of linear forms in logarithms asks whether in the lower bounds established so far the product of the heights of the algebraic numbers can be replaced by their maximum. We have seen that this is indeed the case when the algebraic numbers are very close to 1; see the discussion below Theorem 2.1. This is also not far from being the case when we have several independent small linear relations involving the same logarithms of algebraic numbers. Theorem 9.1 shows that, under this assumption, the product $\log A_1 \cdots \log A_n$ occurring in (1.7) can be replaced by its c-th power, for some real number c with $\frac{1}{n} < c < 1$.

9.1. A theorem of Loxton

The next result was established in 1986 by Loxton [270]. Recall that the naïve height of an algebraic number is the maximum of the absolute values of the coefficients of its minimal defining polynomial over the rational integers.

Theorem 9.1. *Let $n \geq 1$ be an integer and $\alpha_1, \ldots, \alpha_n$ non-zero multiplicatively independent algebraic numbers. Let $t \geq 2$ be an integer and, for $i = 1, \ldots, t$ and $j = 0, \ldots, n$, let $\beta_{i,j}$ be an algebraic number. Consider the linear forms*

$$\Lambda_i = \beta_{i,0} + \beta_{i,1} \log \alpha_1 + \cdots + \beta_{i,n} \log \alpha_n, \quad i = 1, \ldots, t,$$

where log *is the principal determination of the logarithm. Assume that the $t \times (n+1)$ matrix whose entries are the $\beta_{i,j}$ has rank t. Let $B \geq 4$ and, for $j = 1, \ldots, n$, let $A_j \geq 4$ be real numbers such that the naïve height of α_j (resp., of $\beta_{1,j}, \ldots, \beta_{t,j}$) is at most A_j (resp., at most B). Let D be an upper bound for the degree of the field generated by all the α_j and $\beta_{i,j}$. Then, setting*

$$\Omega = \log A_1 \ldots \log A_n,$$

we have

$$\max\{\log |\Lambda_1|, \ldots, \log |\Lambda_t|\} > -(16nD)^{200n} \, (\Omega \, \log \Omega)^{1/t} \, \log \Omega B.$$

This is Theorem 4 in [270]. A result in the same spirit has been obtained by Ramachandra [340] at an early stage of the development of the theory of linear forms in logarithms.

The first estimates for simultaneous linear forms in p-adic logarithms were given by Dong [169]. Subsequently, Gaudron [195] established an explicit lower bound for a system of homogeneous and inhomogeneous linear forms in logarithms of algebraic numbers with algebraic coefficients, both in a complex and in a p-adic framework. His result extends Loxton's estimate.

9.2. Perfect powers in short intervals

Loxton [270] applied Theorem 9.1 to give an upper bound for the number of perfect powers in short intervals.

THEOREM 9.2. *For any sufficiently large integer N, the interval $[N, N + \sqrt{N}]$ contains at most*

$$\exp\big(30\sqrt{\log\log N \log\log\log N}\big)$$

perfect powers.

The interval $[N, N+\sqrt{N}]$ is the appropriate interval to consider in Theorem 9.2, since for any integer $r \geq 2$, it contains at most one r-th power. Furthermore, for any positive real number ε, the interval $[N, N + \sqrt{N} \cdot N^{\varepsilon}]$ contains at least $N^{\varepsilon}(\frac{1}{2} + o(1))$ squares. It is believed that, if N is sufficiently large, then the interval $[N, N + \sqrt{N}]$ contains at most three distinct perfect powers. Actually, the computations in [407] give just one example, namely $11^2, 5^3$, and 2^7, of three prime powers in such an interval.

Loxton's proof of Theorem 9.1 was not complete in the case where the integers he was working with were multiplicatively dependent. Bernstein [62] overcame this difficulty and an alternative proof of Theorem 9.2 was subsequently given by Stewart [398], who also established the following extension of Theorem 9.2, that we state without proof.

THEOREM 9.3. *Let k be an integer with $k \geq 2$. For any sufficiently large integer N, the interval $[N, N + N^{(k-1)/k}]$ contains at most*

$$\exp\big(30\sqrt{\log\log N \log\log\log N}\big)$$

integers which are perfect r-th powers, for some integer $r \geq k$.

Again, the interval $[N, N+N^{(k-1)/k}]$ is the right interval to consider in Theorem 9.3. A more general result of [398] deals with perfect powers of rational numbers in short intervals.

For the proof of Theorem 9.2 we need an auxiliary result, which is Theorem 1 in [398].

LEMMA 9.4. *Let ε be a real number with $0 < \varepsilon < 1$. Let t and k be integers with $t \geq 2$ and*

$$k \geq t\big(1 + \lceil \varepsilon^{-1} \rceil^{t-1}\big). \tag{9.1}$$

If $\alpha_1, \ldots, \alpha_k$ are non-zero algebraic numbers with the property that any t of them are multiplicatively dependent, then there exist distinct indices $i_0, \ldots, i_t$ in $\{1, \ldots, k\}$ for which

$$h\Big(\frac{\alpha_{i_0}}{\alpha_{i_1}}\Big) \leq \varepsilon(h(\alpha_{i_2}) + \cdots + h(\alpha_{i_t})).$$

Proof. By assumption, for every t-tuple $(i_1, \dots, i_t)$ with $1 \le i_1 < i_2 < \cdots < i_t \le k$, there are integers $\ell_{i_1}, \dots, \ell_{i_t}$ not all zero such that

$$\alpha_{i_1}^{\ell_{i_1}} \cdots \alpha_{i_t}^{\ell_{i_t}} = 1.$$

We associate with $(i_1, \dots, i_t)$ the $(t-1)$-tuple obtained by removing the j-th coordinate i_j, where i_j is an index such that $|\ell_{i_j}|$ is maximal, that is,

$$|\ell_{i_j}| \ge |\ell_{i_n}|, \quad \text{for } 1 \le n \le t.$$

Since there are $\binom{k}{t-1}$ $(t-1)$-tuples and $\binom{k}{t}$ different tuples $(i_1, \dots, i_t)$ as above, at least one of the $(t-1)$-tuples is associated with m distinct t-tuples, where

$$m = \left\lceil \binom{k}{t} \Big/ \binom{k}{t-1} \right\rceil = \left\lceil \frac{k-t+1}{t} \right\rceil.$$

Consider one $(t-1)$-tuple with this property. By reordering the α_i's if necessary, we may assume that this $(t-1)$-tuple is $(1, \dots, t-1)$ and the m associated t-tuples are $(1, \dots, t-1, j+t-1)$, for $j = 1, \dots, m$. Let $j = 1, \dots, m$. There are integers $\ell_{1,j}, \dots, \ell_{t-1,j}$ and ℓ_j with $\ell_j > 0$, $|\ell_{1,j}|, \dots, |\ell_{t-1,j}| \le \ell_j$, and

$$\alpha_1^{\ell_{1,j}} \cdots \alpha_{t-1}^{\ell_{t-1,j}} = \alpha_{j+t-1}^{\ell_j}.$$

Put $b_{i,j} = \ell_{i,j}/\ell_j$ for $i = 1, \dots, t-1$. Put $B_j = (b_{1,j}, \dots, b_{t-1,j})$ and observe that B_j is in $[0,1]^{t-1}$. Since, by the assumption (9.1), we have

$$m > \lceil \varepsilon^{-1} \rceil^{t-1},$$

it follows from Dirichlet's *Schubfachprinzip* that there exist two $(t-1)$-tuples B_u and B_s with $1 \le u < s \le m$ whose entries satisfy

$$|b_{i,u} - b_{i,s}| \le \varepsilon, \quad \text{for } i = 1, \dots, t-1. \tag{9.2}$$

Since

$$\alpha_1^{\ell_s \ell_{1,u} - \ell_u \ell_{1,s}} \cdots \alpha_{t-1}^{\ell_s \ell_{t-1,u} - \ell_u \ell_{t-1,s}} = \Big(\frac{\alpha_{u+t-1}}{\alpha_{s+t-1}}\Big)^{\ell_u \ell_s},$$

we get

$$\ell_u \ell_s h\Big(\frac{\alpha_{u+t-1}}{\alpha_{s+t-1}}\Big) \le \sum_{i=1}^{t-1} |\ell_s \ell_{i,u} - \ell_u \ell_{i,s}|\, h(\alpha_i),$$

by Theorem B.5. We conclude by (9.2) that

$$h\Big(\frac{\alpha_{u+t-1}}{\alpha_{s+t-1}}\Big) \le \varepsilon \sum_{i=1}^{t-1} h(\alpha_i).$$

This proves the lemma. □

Proof of Theorem 9.2. Let $N \geq 100$ be an integer and put

$$t = \left\lceil \frac{1}{15}\sqrt{\frac{\log\log N}{\log\log\log N}} \right\rceil, \quad L = t(1 + (9(t-1))^{t-1}),$$

and

$$M = \exp\bigl(29\sqrt{\log\log N \log\log\log N}\bigr).$$

Suppose that there are positive integers $x_1, \dots, x_L, b_1, \dots, b_L$ with $\min\{b_1, \dots, b_L\} \geq M$ such that $x_1^{b_1}, \dots, x_L^{b_L}$ are distinct and lie in the interval $[N, N + \sqrt{N}]$. Assume that any t integers among $x_1^{b_1}, \dots, x_L^{b_L}$ are multiplicatively dependent. Then, by Lemma 9.4 applied with $\varepsilon = (9(t-1))^{-1}$, there exist distinct indices $i_0, \dots, i_t$ for which

$$\frac{\max\{x_{i_0}^{b_{i_0}}, x_{i_1}^{b_{i_1}}\}}{\gcd(x_{i_0}^{b_{i_0}}, x_{i_1}^{b_{i_1}})} = \exp h\left(\frac{x_{i_0}^{b_{i_0}}}{x_{i_1}^{b_{i_1}}}\right) \leq \bigl(x_{i_2}^{b_{i_2}} \cdots x_{i_t}^{b_{i_t}}\bigr)^{\varepsilon} \leq (2N)^{\varepsilon(t-1)} = \sqrt[9]{2N}. \tag{9.3}$$

Since the integers $x_{i_0}^{b_{i_0}}$ and $x_{i_1}^{b_{i_1}}$ are lying in the interval $[N, N + \sqrt{N}]$, their greatest prime divisor cannot exceed $\sqrt{N}$. Consequently, the left hand side of (9.3) is at least equal to $\sqrt{N}$ and we have derived a contradiction since $N \geq 4$.

Thus, by reordering the powers, we may assume, without any loss of generality, that $x_1^{b_1}, \dots, x_t^{b_t}$ are multiplicatively independent and that $b_i < b_t$ for $i = 1, \dots, t-1$. Put

$$\Lambda_i := b_i \log x_i - b_t \log x_t, \quad i = 1, \dots, t-1,$$

and observe that

$$|\Lambda_i| = \left|\log \frac{x_i^{b_i}}{x_t^{b_t}}\right| \leq \log\Bigl(1 + \frac{1}{\sqrt{N}}\Bigr) < \frac{1}{\sqrt{N}}, \quad i = 1, \dots, t-1. \tag{9.4}$$

It follows from Theorem 2.2 that

$$\log|\Lambda_i| > -10^{10}\,(\log x_i)(\log x_t)(\log b_t), \quad i = 1, \dots, t-1,$$

and, using that

$$x_j \leq (2N)^{1/b_j} \leq N^{2/M}, \quad j = 1, \dots, t, \tag{9.5}$$

we get

$$\log|\Lambda_i| > -10^{10}\,(\log N^{2/M})^2(\log b_t), \quad i = 1, \dots, t-1. \tag{9.6}$$

Since $x_1, \dots, x_t$ are multiplicatively independent and the $(t-1) \times t$ matrix

$$\begin{pmatrix} b_1 & 0 & \cdots & 0 & -b_t \\ 0 & & & & \vdots \\ \vdots & & & & \vdots \\ 0 & \cdots & 0 & b_{t-1} & -b_t \end{pmatrix}$$

has rank $t-1$, we can apply Theorem 9.1 to show that the lower bound (9.6) can be considerably improved (when N is large) for (at least) one of the quantities $|\Lambda_1|, \dots, |\Lambda_{t-1}|$. Indeed, since $b_t \ge M \ge 4$, it follows from Theorem 9.1 and (9.5) that

$$\begin{aligned}&\log\max\{|\Lambda_1|, \dots, |\Lambda_{t-1}|\}\\ &\quad > -(16t)^{200t}\bigl(\log N^{2/M}\bigr)^{t/(t-1)}\bigl(t\log\log N^{2/M}\bigr)^{1/(t-1)}\log\bigl(\bigl(\log N^{2/M}\bigr)^t b_t\bigr).\end{aligned}$$

Combined with (9.4) and the upper bound $b_t \le \frac{2\log N}{\log 2} < 4\log N$, we then get

$$\begin{aligned}\log N &< 2(16t)^{200t}\Bigl(t\Bigl(\frac{2\log N}{M}\Bigr)^t\log\Bigl(\frac{2\log N}{M}\Bigr)\Bigr)^{1/(t-1)}\log\Bigl(4(\log N)\Bigl(\frac{2\log N}{M}\Bigr)^t\Bigr)\\ &\le 2(t+1)(16t)^{200t}\Bigl(t\Bigl(\frac{2\log N}{M}\Bigr)^t\log(2\log N)\Bigr)^{1/(t-1)}\log(4\log N),\end{aligned}$$

which gives

$$M < (16t)^{200t}(\log N)^{1/t}\log(4\log N).$$

By the definitions of t and M, this cannot happen if N is large enough. Consequently, the interval $[N, N+\sqrt{N}]$ contains at most L integers of the form x^r with $r \ge M$. Furthermore, as already noticed, for any integer r with $r \ge 2$, the interval $[N, N+\sqrt{N}]$ contains at most one r-th power. We conclude that the total number of perfect powers in $[N, N+\sqrt{N}]$ is at most equal to $L+M$. This completes the proof. □

9.3. Simultaneous Pellian equations with at most one solution

Our second application of Loxton's result, which was obtained by Bennett and Pintér [58], gives a quantitative upper bound for the number of solutions to certain systems of Pellian equations. Classical results on quadratic fields are given in Appendix C. Recall that the fundamental unit of a real quadratic field K is the unit η in K such that $\eta > 1$ and any unit in K can be written $\pm\eta^m$, where m is a rational integer.

THEOREM 9.5. *Let a and b be non-square positive integers and let ε_a and ε_b denote the fundamental units in $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, respectively. There exists an effectively computable real number $\kappa > 1$ such that, if*

$$\log\varepsilon_b \ge \kappa(\log a)(\log\varepsilon_a)(\log\log(2a\varepsilon_a))^3, \tag{9.7}$$

then the system of simultaneous Pellian equations

$$|x^2 - ay^2| = |y^2 - bz^2| = 1 \tag{9.8}$$

has at most one solution in positive integers x, y, and z.

Proceeding as in the proof of Theorem 3.13, it is easy to show that, for any given non-square positive integers a, b, the equations (9.8) have only finitely many solutions in integers x, y, z.

In [58] the factor $\log\log(2a\varepsilon_a)$ in (9.7) is replaced by $\log\log(3\varepsilon_a)$. The authors overlooked in their proof that a can be much larger than ε_a, a case which may occur when a has a large square factor. The result of [58] addresses, more generally, intersection of recurrence sequences having a dominant root (the authors assumed that this root is simple, but their argument also works if this is not the case).

Proof. Let denote by ε_a^σ and ε_b^σ the Galois conjugates of ε_a and ε_b, respectively. Note that

$$h(\varepsilon_a) = \frac{\log \varepsilon_a}{2}, \quad h(\varepsilon_b) = \frac{\log \varepsilon_b}{2}, \quad \text{and} \quad \varepsilon_a, \varepsilon_b \geq \frac{1+\sqrt{5}}{2}.$$

Assume that (9.7) holds for some $\kappa > 1$ and that Equation (9.8) has two solutions in positive integers, say (x_1, y_1, z_1) and (x_2, y_2, z_2), with $x_1 < x_2$. Then, there are positive integers m_1, m_2, n_1, and n_2 such that

$$y_i = \frac{\varepsilon_a^{n_i} - (\varepsilon_a^\sigma)^{n_i}}{2\sqrt{a}} = \frac{\varepsilon_b^{m_i} + (\varepsilon_b^\sigma)^{m_i}}{2}, \quad i = 1, 2.$$

Let $i = 1, 2$. Observe that

$$\frac{\varepsilon_a^{n_i}}{2\sqrt{a}} \neq \frac{\varepsilon_b^{m_i}}{2}, \quad n_i \geq 2m_i, \quad \text{and} \quad |\varepsilon_b^{m_i} \varepsilon_a^{-n_i} \sqrt{a} - 1| \leq 1.1 \varepsilon_a^{-2n_i}, \tag{9.9}$$

by (9.7). It follows from (9.7) and (9.9) that the linear form

$$\Lambda_i := m_i \log \varepsilon_b - n_i \log \varepsilon_a + \log \sqrt{a}$$

satisfies

$$\log |\Lambda_i| < \log 2.2 - 2n_i \log \varepsilon_a < -\frac{\log \varepsilon_b}{2}. \tag{9.10}$$

By (9.7), the fundamental units ε_a and ε_b are distinct. Thus, the three algebraic numbers $\varepsilon_a, \varepsilon_b, \sqrt{a}$ are multiplicatively independent. By applying Theorem 2.2, we get from (9.9) that

$$\log |\Lambda_i| \gg -(\log a)(\log \varepsilon_a)(\log \varepsilon_b)(\log 2n_i).$$

We conclude that

$$n_i \ll (\log a)(\log \varepsilon_b)(\log 2n_i),$$

thus, by (9.7),

$$n_i \ll (\log a)(\log \varepsilon_b)(\log \log 2\varepsilon_b). \tag{9.11}$$

The matrix

$$\begin{pmatrix} m_1 & -n_1 & 1 \\ m_2 & -n_2 & 1 \end{pmatrix}$$

has rank two. Observe that the naïve height of ε_a is equal to $\varepsilon_a + \varepsilon_a^\sigma$, thus is less than $2\varepsilon_a$. Likewise, the naïve height of ε_b is less than $2\varepsilon_b$. By Theorem 9.1 applied with the quantity

$$\Omega = (\log 2a)(\log 3\varepsilon_a)(\log 3\varepsilon_b),$$

we deduce from (9.11) that

$$\begin{aligned} \max\{\log|\Lambda_1|, \log|\Lambda_2|\} &\gg -(\Omega \log \Omega)^{1/2} \log \max\{n_1\Omega, n_2\Omega\} \\ &\gg -\Omega^{1/2} (\log \Omega)^{3/2}. \end{aligned}$$

Combining this with (9.10) and (9.7), we get

$$\log \varepsilon_b \ll \Omega^{1/2}(\log \Omega)^{3/2} \ll (\log a)^{1/2}(\log \varepsilon_a)^{1/2}(\log \varepsilon_b)^{1/2}(\log\log \varepsilon_b)^{3/2},$$

whence

$$\log \varepsilon_b \ll (\log a)(\log \varepsilon_a)(\log\log \varepsilon_b)^3.$$

This shows that the system (9.8) cannot have two solutions if κ in (9.7) is taken sufficiently large. This completes the proof of the theorem. □

9.4. Exercise

Exercise 9.1 (Continuation of Exercise 3.7; see [104]). Use (3.36) and Theorem 9.1 to prove that, if a, b, c are positive integers with $a \geq b > c$, then

$$P[a(ab+1)(bc+1)(ca+1)] \gg \log\log a.$$

[Hint. Consider the quantities $\Lambda_1 := \frac{ac+1}{ac} - 1$ and $\Lambda_2 := \frac{(ac+1)(bc+1)}{c^2(ab+1)} - 1$].

9.5. Notes

▹ Theorem 9.1 has been applied to Thue equations by Brindza [94], to unit equations by Brindza and Győry [96], and to sets of integers whose shifted products are powers by Stewart [397]; see the Notes at the end of Chapter 5.

▹ It does not seem that any application of simultaneous linear forms in p-adic logarithms has been found yet.

▹ Corvaja and Zannier [157] and, independently and simultaneously, Hernández and Luca [226] applied the Schmidt subspace theorem to show that the greatest prime factor of $(ab+1)(bc+1)(ca+1)$ tends to infinity as the maximum of the pairwise distinct positive integers a, b, c tends to infinity. Actually, a stronger result is proved in [157], namely that the greatest prime factor of $(ab+1)(ac+1)$ tends to infinity as the maximum of the pairwise distinct positive integers a, b, and c goes to infinity; see also [130].

Chapter 10

Multiplicative dependence relations between algebraic numbers

By definition, if $\alpha_1, \ldots, \alpha_m$ are multiplicatively dependent algebraic numbers, then there exist integers $n_1, \ldots, n_m$ not all zero such that $\alpha_1^{n_1} \cdots \alpha_m^{n_m} = 1$. The main aim of this chapter is to show that $n_1, \ldots, n_m$ can be chosen not too large in absolute value.

We largely follow the presentation of Waldschmidt [432] and begin with a brief study of lower bounds for the height of an algebraic number expressed in terms of its degree.

10.1. Lower bound for the height of an algebraic number

By definition of the height, if α is zero or a root of unity, then its height is equal to zero. Kronecker's Theorem B.6 asserts that these are the only algebraic numbers whose height is zero. The next theorem, used in the proof of Theorem 10.5 and in various other parts of this monograph, gives an explicit version of Theorem B.6.

Theorem 10.1. *Let d be a positive integer and α a non-zero algebraic number of degree at most d. If α is not a root of unity, then*

$$h(\alpha) > \frac{1}{11d^3}.$$

A much larger lower bound for $h(\alpha)$ than the one given in Theorem 10.1 is known. Namely, Louboutin [269] established that, for every positive real number ε, there exists an integer $d_0(\varepsilon)$ such that every algebraic number of degree d greater than $d_0(\varepsilon)$, and which is not a root of unity, satisfies

$$h(\alpha) > \frac{9-\varepsilon}{4d}\left(\frac{\log\log d}{\log d}\right)^3. \tag{10.1}$$

This slight improvement of a seminal theorem of Dobrowolski [167] is currently the best known result towards the celebrated *Lehmer problem*.

Problem 10.2 (Lehmer's problem). *To prove or to disprove that there exists a positive absolute real number c such that every non-zero algebraic number α which is not a root of unity satisfies*

$$h(\alpha) > \frac{c}{\deg(\alpha)}.$$

A comprehensive list of partial results towards Lehmer's problem is given in Section 3.6 of [432]; see also [143,306,383] and Chapter 16 of [287] for a complete proof of a slightly weaker lower bound than (10.1).

We need two auxiliary lemmas for the proof of Theorem 10.1. The first one is the following consequence of Fermat's little theorem.

Lemma 10.3. *Let p be a prime number and $f(X_1, \dots, X_k)$ a polynomial in k variables with integer coefficients. Then, every coefficient of the polynomial*

$$f(X_1^p, \dots, X_k^p) - f(X_1, \dots, X_k)^p$$

is divisible by p.

Proof. For non-negative integers $i_1, \dots, i_k$ and a non-zero integer a, the desired result holds for the monomial $aX_1^{i_1} \cdots X_k^{i_k}$, since p divides the integer $a - a^p$. Let $f_1(X_1, \dots, X_k)$ and $f_2(X_1, \dots, X_k)$ be integer polynomials such that every coefficient of the polynomials

$$f_1(X_1^p, \dots, X_k^p) - f_1(X_1, \dots, X_k)^p \quad \text{and} \quad f_2(X_1^p, \dots, X_k^p) - f_2(X_1, \dots, X_k)^p$$

is divisible by p. Observe that the coefficients of the polynomial

$$(f_1 + f_2)^p - f_1^p - f_2^p = \sum_{h=1}^{p-1} \binom{p}{h} f_1^h f_2^{p-h}$$

are rational integers which are all divisible by p. Consequently, every coefficient of the polynomial

$$(f_1 + f_2)(X_1^p, \dots, X_k^p) - \big((f_1 + f_2)(X_1, \dots, X_k)\big)^p$$

is a multiple of p. The lemma follows by linearity. □

We further need an easy lemma on roots of unity.

Lemma 10.4. *Let α be a non-zero algebraic number. Assume that there exist two distinct positive integers h and ℓ such that α^h and α^ℓ are Galois conjugate. Then α is a root of unity.*

Proof. Let K be the number field generated over $\mathbb{Q}$ by α and its Galois conjugates. From the assumption that α^h and α^ℓ are conjugate, we deduce that there exists an element φ in the Galois group of K over $\mathbb{Q}$ such that $\varphi(\alpha^h) = \alpha^\ell$. By induction, we establish that $\varphi^n(\alpha^{h^n}) = \alpha^{\ell^n}$ for $n \geq 1$. Denoting by m the order of φ in the Galois group of K over $\mathbb{Q}$, we deduce that $\alpha^{h^m} = \alpha^{\ell^m}$. Since h and ℓ are distinct, we conclude that α is a root of unity. □

Proof of Theorem 10.1. Let α be a non-zero algebraic number of degree d. If α is not an algebraic integer, then its height is at least equal to $\frac{\log 2}{d}$. Consequently, there is no restriction in assuming that α is an algebraic integer. Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ denote its Galois conjugates. Let ℓ be a positive integer and p a prime number. The sum

$$S_\ell = \alpha_1^\ell + \cdots + \alpha_d^\ell$$

(which is the *trace* of α^ℓ from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$) is a rational integer. By Fermat's little theorem, S_ℓ and S_ℓ^p are congruent modulo p. Furthermore, by applying Lemma 10.3 with $k = d$ for the polynomial $f_\ell = X_1^\ell + \cdots + X_d^\ell$, we deduce that there exists an integer polynomial $g_\ell(X_1, \ldots, X_d)$ such that

$$S_{\ell p} - S_\ell^p = p \cdot g_\ell(\alpha_1, \ldots, \alpha_d).$$

Since $g_\ell(\alpha_1, \ldots, \alpha_d)$ is an algebraic integer, it must be a rational integer and we deduce that $S_{\ell p}$ and S_ℓ^p are congruent modulo p. This shows that the three integers $S_{\ell p}$, S_ℓ, and S_ℓ^p are congruent modulo p. Recalling that, for $j = 1, \ldots, d$,

$$h(\alpha) = \frac{1}{d} \sum_{h=1}^{d} \log \max\{1, |\alpha_h|\} \geq \frac{1}{d} \log \max\{1, |\alpha_j|\},$$

we get $|\alpha_j| \leq \mathrm{e}^{dh(\alpha)}$, hence

$$|S_\ell| \leq d\ \mathrm{e}^{\ell d h(\alpha)}.$$

We now assume $\mathrm{e}^{dh(\alpha)} \leq 1 + 1/(4\mathrm{e}d^2)$. By Theorem D.1, we may assume that the prime number p satisfies $2\mathrm{e}d < p < 4\mathrm{e}d$. For $\ell = 1, \ldots, d$, the estimates

$$|S_\ell| \leq d\Big(1 + \frac{1}{4\mathrm{e}d^2}\Big)^d \leq d\mathrm{e} \quad \text{and} \quad |S_{\ell p}| \leq d\Big(1 + \frac{1}{4\mathrm{e}d^2}\Big)^{4\mathrm{e}d^2} \leq d\mathrm{e}$$

imply that

$$|S_\ell - S_{\ell p}| \leq 2d\mathrm{e} < p.$$

Since S_ℓ and $S_{\ell p}$ are congruent modulo p, it follows that $S_\ell = S_{\ell p}$ for $\ell = 1, \ldots, d$. This implies that α and α^p have the same minimal defining polynomial, thus they are Galois conjugates. We then deduce from Lemma 10.4 that α is a root of unity.

Consequently, if α is a non-zero algebraic number which is not a root of unity, then $\mathrm{e}^{dh(\alpha)} > 1 + 1/(4\mathrm{e}d^2)$. Noticing that the inequality

$$\Big(1 + \frac{1}{4\mathrm{e}d^2}\Big)^{11d^2} > \mathrm{e}$$

holds for $d \geq 2$, we deduce that

$$h(\alpha) \geq \frac{1}{d} \log\Big(1 + \frac{1}{4\mathrm{e}d^2}\Big) > \frac{1}{11d^3}.$$

This completes the proof of Theorem 10.1. □

10.2. Existence of small multiplicative dependence relations

The main result of this section is the following theorem.

THEOREM 10.5. *Let $m \geq 2$ be an integer and $\alpha_1, \dots, \alpha_m$ multiplicatively dependent non-zero algebraic numbers. Let $\log\alpha_1, \dots, \log\alpha_m$ be any determination of their logarithms. Let D be the degree of the number field generated by $\alpha_1, \dots, \alpha_m$ over $\mathbb{Q}$. For $j = 1, \dots, m$, let A_j be a real number satisfying*

$$\log A_j \geq \max\Big\{h(\alpha_j), \frac{|\log\alpha_j|}{D}, 1\Big\}.$$

Then, there exist integers $n_1, \dots, n_m$, not all zero, such that

$$n_1\log\alpha_1 + \cdots + n_m\log\alpha_m = 0, \quad \alpha_1^{n_1}\cdots\alpha_m^{n_m} = 1,$$

and

$$|n_k| \leq \big(11(m-1)D^3\big)^{m-1}\frac{(\log A_1)\cdots(\log A_m)}{\log A_k}, \quad \textit{for } k = 1, \dots, m. \tag{10.2}$$

Let $\alpha_1, \dots, \alpha_m$ be multiplicatively dependent algebraic numbers. The set G of integer m-tuples $(n_1, \dots, n_m)$ such that $\alpha_1^{n_1}\cdots\alpha_m^{n_m} = 1$ is a subgroup of $\mathbb{Z}^m$ of rank at least one. Theorem 10.5 provides us with an upper bound for the first minimum of the discrete subgroup G in $\mathbb{R}^m$.

Matveev [289,292] proved that the factor $\big(11(m-1)D^3\big)^{m-1}$ in (10.2) can be replaced by $C^m D\log D$, for some absolute real number C; see also Loher and Masser [267] and Loxton and van der Poorten [271].

Proof. We assume, as we may without loss of generality, that $m \geq 2$, and that any $m-1$ elements among $\alpha_1, \dots, \alpha_m$ are multiplicatively independent. Thus there exists a unique (up to a factor ± 1) set of relatively prime non-zero integers $n_1, \dots, n_m$ such that

$$n_1\log\alpha_1 + \cdots + n_m\log\alpha_m = 0.$$

Fix an integer k with $1 \leq k \leq m$. Define $c_1, \dots, c_m$ by

$$c_j = \big(11(m-1)D^3\log A_j\big)^{-1}, \quad 1 \leq j \leq m, \; j \neq k,$$

and

$$c_k = \big(11(m-1)D^3\big)^{m-1}\prod_{\substack{1\leq j\leq m,\\ j\neq k}}\log A_j,$$

in such a way that $c_1\cdots c_m = 1$. Using Minkowski's theorem (see e.g. [357, Chapter II] or [113, Appendix B]), we deduce that there exist integers $\nu_1, \dots, \nu_m$, not all zero, such that

$$\left|\nu_j - \frac{\nu_k n_j}{n_k}\right| \leq c_j, \quad 1 \leq j \leq m, \; j \neq k, \quad \text{and} \quad |\nu_k| \leq c_k.$$

In order to prove the relation $\nu_1\log\alpha_1 + \cdots + \nu_m\log\alpha_m = 0$, we first show that the number $\alpha = \alpha_1^{\nu_1}\cdots\alpha_m^{\nu_m}$ is a root of unity. Observe that the number

$$\alpha^{n_k} = \prod_{j=1}^{m}\alpha_j^{\nu_j n_k} = \prod_{j=1}^{m}\alpha_j^{\nu_j n_k - \nu_k n_j}$$

satisfies

$$|n_k|\, h(\alpha) \le \sum_{\substack{1\le j\le m,\\ j\ne k}} |\nu_j n_k - \nu_k n_j|\, h(\alpha_j),$$

hence

$$h(\alpha) \le \sum_{\substack{1\le j\le m,\\ j\ne k}} c_j h(\alpha_j) \le \frac{m-1}{11(m-1)D^3} = \frac{1}{11D^3}.$$

It then follows from Theorem 10.1 that α is a root of unity. Let M be the smallest positive integer such that $\alpha^M = 1$. Then, α is a primitive M-th root of unity, hence of degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(M)$ over $\mathbb{Q}$, where φ denotes Euler's totient function. Write $M = q_1^{u_1} \cdots q_r^{u_r}$, where $q_1, \ldots, q_r$ are distinct prime numbers and $u_1, \ldots, u_r$ are positive integers. Then,

$$\varphi(M) = q_1^{u_1-1}(q_1-1)\cdots q_r^{u_r-1}(q_r-1)$$

and

$$\frac{\varphi(M)}{\sqrt{M}} = q_1^{(u_1-2)/2}(q_1-1)\cdots q_r^{(u_r-2)/2}(q_r-1) \ge \frac{q_1-1}{\sqrt{q_1}}\cdots\frac{q_r-1}{\sqrt{q_r}} \ge \frac{1}{\sqrt{2}}.$$

Since the degree of α is at most equal to D, we get $\varphi(M) \le D$, giving that $M \le 2D^2$ (note that sharper estimates hold; see Exercise 7.2.a of [432]) and

$$M\sum_{j=1}^{m} \nu_j \log\alpha_j \quad \text{is in } 2i\pi\mathbb{Z}. \tag{10.3}$$

Observe that

$$\begin{aligned}\Big|M\sum_{j=1}^{m} \nu_j \log\alpha_j\Big| &= \Big|M\sum_{j=1}^{m} \Big(\nu_j - \frac{\nu_k n_j}{n_k}\Big)\log\alpha_j\Big|\\ &\le M \sum_{\substack{1\le j\le m,\\ j\ne k}} c_j |\log\alpha_j| \le \frac{M}{11D^2} \le \frac{2}{11} < 2\pi.\end{aligned}$$

Combined with (10.3), this shows that

$$\sum_{i=1}^{m} \nu_j \log\alpha_j = 0.$$

Therefore, there exists a non-zero rational integer ℓ such that $(\nu_1, \ldots, \nu_m) = (\ell n_1, \ldots, \ell n_m)$. We deduce the inequality $|n_k| \le |\nu_k|$, from which the desired upper bound $|n_k| \le c_k$ readily follows. □

Chapter 11
Lower bounds for linear forms in two complex logarithms: proofs

The purpose of this chapter is to present complete proofs of versions of Theorems 2.3, 2.4, and 2.6, with the same dependence in all the parameters, but with larger numerical constants. Not to focus on the size of these constants allows some simplification in the proofs.

11.1. Three estimates for linear forms in two complex logarithms

Let α_1, α_2 be non-zero complex algebraic numbers and $\log \alpha_1, \log \alpha_2$ any determinations of their logarithms. Set $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$. Let A_1, A_2 be real numbers with

$$\log A_j \geq \max\Bigl\{h(\alpha_j), \frac{|\log \alpha_j|}{D}, \frac{1}{D}\Bigr\}, \quad j = 1, 2.$$

Let b_1, b_2 be non-zero integers such that $b_1 \log \alpha_1 + b_2 \log \alpha_2$ is non-zero and set

$$B' = \frac{|b_1|}{D \log A_2} + \frac{|b_2|}{D \log A_1}.$$

Theorem 11.1. *Under the above notation and assumption, we have the lower bound*

$$\log |b_1 \log \alpha_1 + b_2 \log \alpha_2| \geq -21600\, D^4 (\log A_1)(\log A_2)(\max\{10, \log B'\})^2.$$

A complete proof of a version of Theorem 11.1 when α_1 and α_2 are real numbers was given by Laurent [252]; see also [253, 254] for the complex case and some improvements.

As will be apparent in its proof, Theorem 11.1 can be considerably sharpened when α_1 and α_2 are both real numbers very close to 1.

Theorem 11.2. *Keep the above notation and assumption. Suppose furthermore that α_1 and α_2 are real numbers greater than 1 and set*

$$E = 1 + \min\Bigl\{\frac{D \log A_1}{\log \alpha_1}, \frac{D \log A_2}{\log \alpha_2}\Bigr\}.$$

Assume that $E \leq \min\{A_1^{3D/2}, A_2^{3D/2}\}$. Then, we have the lower bound

$$\log |b_1 \log \alpha_1 + b_2 \log \alpha_2| \geq -78500\, D^4 \frac{(\log A_1)(\log A_2)}{\log E} \Bigl(\max\Bigl\{\frac{3}{D}, \frac{\log B'}{\log E}\Bigr\}\Bigr)^2.$$

By taking $E = 2$ in Theorem 11.2, we get a slightly weaker version of Theorem 11.1.

Unlike in Theorem 2.3, we do not assume in Theorem 11.1 that α_1 and α_2 are multiplicatively independent. In particular, Theorem 11.1 applied with $\alpha_1 = -1$ and $\log A_1 = \frac{\pi}{D}$ implies the following result, which is similar to Theorem 2.6.

Theorem 11.3. *Let α be an algebraic number on the unit circle and which is not a root of unity. Let D be its degree and A a real number such that*

$$\log A \geq \max\Big\{h(\alpha), \frac{|\log\alpha|}{D}, \frac{1}{D}\Big\}.$$

Let b_1, b_2 be non-zero integers and set

$$B' = \frac{|b_1|}{D\log A} + \frac{|b_2|}{\pi}.$$

Then,

$$\log|b_1 \mathrm{i}\pi - b_2\log\alpha| \geq -68000\, D^3(\log A)(\max\{10, \log B'\})^2.$$

Apart from the value of the numerical constant, Theorem 11.3 is as strong as Theorem 2.6.

11.2. An auxiliary inequality involving several parameters

For convenience, we slightly change the notation of Theorem 11.1. Without loss of generality, we assume that b_1 and b_2 are positive and that the moduli of α_1 and α_2 are at least equal to 1. We then write in all what follows

$$\Lambda = b_2 \log\alpha_2 - b_1 \log\alpha_1.$$

This is not restrictive. Indeed, if $|\alpha_1|$ and $|\alpha_2|$ are both less than 1, then replacing α_1 and α_2 by their inverses does not affect $|\Lambda|$. Also, if $|\alpha_1| < 1$ and $|\alpha_2| > 1$, then the real part of Λ is the sum of two positive terms and can easily be bounded using Liouville's inequality Theorem B.10. Furthermore, by permuting the indices 1 and 2 if necessary, we can suppose that

$$b_1|\log\alpha_1| \leq b_2|\log\alpha_2|. \tag{11.1}$$

We keep this assumption until the end of this chapter.

Theorem 11.4. *Let $K \geq 3$, L, R_1, R_2, S_1, and S_2 be integers at least equal to 2. Set $N = KL$, $R = R_1 + R_2 - 1$, and $S = S_1 + S_2 - 1$. Assume that the conditions*

$$\mathrm{Card}\{\alpha_1^r\alpha_2^s : 0 \leq r < R_1,\ 0 \leq s < S_1\} \geq L, \tag{11.2}$$

$$\mathrm{Card}\{rb_2 + sb_1 : 0 \leq r < R_2,\ 0 \leq s < S_2\} > (K-1)L \tag{11.3}$$

are satisfied. Set

$$b = \big((R-1)b_2 + (S-1)b_1\big)\Bigg(\prod_{k=1}^{K-1} k!\Bigg)^{-2/(K^2-K)}. \tag{11.4}$$

Let $\rho > 1$ be a real number. If the inequality

$$
\begin{aligned}
(N-K)\,\log\rho > {} & 2(D+1)\log N + (D+1)K\log b \\
& + 2LR\bigl(\rho\,|\log\alpha_1| + D\,h(\alpha_1)\bigr) + 2LS\bigl(\rho\,|\log\alpha_2| + D\,h(\alpha_2)\bigr)
\end{aligned}
\tag{11.5}
$$

holds, then we have

$$
|\Lambda|\,\max\left\{\frac{\mathrm{e}^{|\Lambda|LR/b_1}LR}{b_1}, \frac{\mathrm{e}^{|\Lambda|LS/b_2}LS}{b_2}\right\} > \rho^{-N}.
$$

Theorem 11.4 is slightly weaker than Théorème 1 of [254]. The next section is devoted to its proof. Then, we deduce Theorems 11.1 and 11.2 from Theorem 11.4 in Sections 11.4 and 11.5.

Let us briefly discuss (11.5) and convince the reader that it can be satisfied, even for large values of ρ. Assume for convenience that α_1 or α_2 is not a root of unity. Then, (11.2) holds for $R_1 = S_1 = L$. Assuming that $K \ge L > 10$, we see that (11.5) holds if

$$
\begin{aligned}
K(L-1)\,\log\rho > {} & 2(D+1)K\log b \\
& + 2(\rho+1)DL\bigl((L+R_2)\log A_1 + (L+S_2)\log A_2\bigr).
\end{aligned}
\tag{11.6}
$$

This forces L to be $\gg D\log b$. By assumption (11.3), the product R_2S_2 exceeds $K(L-1)$. Thus, the left hand side of (11.6) involves the product R_2S_2, while its right hand side is linear in R_2 and S_2. This shows that (11.6) can be satisfied, even for large values of ρ. For instance, we can take

$$
R_2 \gg \rho DL(\log A_2), \quad S_2 \gg \rho DL(\log A_1), \quad \text{and} \quad K \gg \rho^2D^2L(\log A_1)(\log A_2),
$$

keeping in mind that the conclusion of Theorem 11.4 is better when KL is small.

To replace (11.5) by (11.6), we have bounded $\rho|\log\alpha_1|$ (*resp.*, $\rho|\log\alpha_2|$) from above by $\rho D\log A_1$ (*resp.*, $\rho D\log A_2$). If α_1 and α_2 are real numbers greater than 1, then, by taking ρ equal to the quantity E defined in Theorem 11.2, we get the stronger upper bounds $\rho\log\alpha_1 \le 2D\log A_1$ and $\rho\log\alpha_2 \le 2D\log A_2$, showing that the factor $2(\rho+1)$ occurring in (11.6) can then be replaced by 6. For large values of ρ, the inequality

$$
K(L-1)\,\log\rho > 2(D+1)K\log b + 6DL\bigl((L+R_2)\log A_1 + (L+S_2)\log A_2\bigr).
$$

is clearly much easier to be satisfied than (11.6). This roughly explains why the lower bound in Theorem 11.1 can be considerably improved when the parameter E can be taken to be large.

11.3. Proof of Theorem 11.4

We keep the notation of Section 11.2 and Theorem 11.4. Assume that the inequalities (11.2) and (11.3) are satisfied. Observe that

$$
RS \ge R_1S_1 + R_2S_2 > KL.
$$

It follows from Lemma E.1, applied with

$$\mathcal{E} = \{(r,s) : 0 \le r < R_1,\ 0 \le s < S_1\}$$

and

$$\mathcal{E}' = \{(r',s') : 0 \le r' < R_2,\ 0 \le s' < S_2\},$$

that the $KL \times RS$ matrix $\mathcal{M}$ whose coefficients are the complex numbers

$$\binom{rb_2 + sb_1}{k} {\alpha_1}^{\ell r} {\alpha_2}^{\ell s}$$

is of maximal rank, equal to $N = KL$. To see this, observe that if the KL lines of $\mathcal{M}$ were linearly dependent, then there would exist a non-zero integer polynomial $P(X,Y)$, whose degree in X is at most $K-1$ and whose degree in Y is at most $L-1$, vanishing at all the points $(rb_2 + sb_1, \alpha_1^r \alpha_2^s)$ with $0 \le r < R, 0 \le s < S$. This would contradict Lemma E.1.

Thus, we can extract from $\mathcal{M}$ a non-zero minor Δ of size $N \times N$, which can be written, with a suitable ordering of the columns,

$$\Delta = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} {\alpha_1}^{\ell_i r_j} {\alpha_2}^{\ell_i s_j} \right)_{1 \le i,j \le N}.$$

We index the lines by pairs (k,ℓ) and the columns by pairs (r,s). For convenience, we fix the numbering of the lines by using the formulas

$$k_i = i - 1 - K\lfloor (i-1)/K \rfloor, \quad \ell_i = \lfloor (i-1)/K \rfloor, \quad \text{for } i = 1, \ldots, KL.$$

The columns are indexed by the N distinct pairs of integers $(r_1,s_1), \ldots, (r_N,s_N)$, where $0 \le r_j < R$ and $0 \le s_j < S$ for $j = 1, \ldots, N$. In the sequel, we will use repeatedly that, for any permutation σ of the set $\{1,\ldots,N\}$, we have

$$\sum_{i=1}^{N} \ell_i r_{\sigma(i)} \le LRN \quad \text{and} \quad \sum_{i=1}^{N} \ell_i s_{\sigma(i)} \le LSN. \tag{11.7}$$

We stress that it is very important to use, in the definition of the determinant Δ, the binomial coefficients $\binom{rb_2+sb_1}{k}$, and not the integers $(rb_2 + sb_1)^k$. Indeed, otherwise, we would have to take b equal to $Rb_2 + Sb_1$ and we would ultimately get a weaker version of Theorem 11.1 with, in particular, B' replaced by $\max\{3, |b_1|, |b_2|\}$. The idea to use binomial coefficients rather than integral powers goes back to Feldman [185].

The strategy of the proof goes as follows. Recall that, by construction, Δ is non-zero. We bound $|\Delta|$ from below by means of Liouville's inequality (Theorem B.10) and from above using complex analysis (namely, the maximum principle). Then, we show that the lower bound exceeds the upper bound if $|\Lambda|$ is small enough. This contradiction implies that $|\Lambda|$ cannot be too small.

As explained in [252], the determinant Δ is the interpolation determinant of the N functions in the two variables x, y,

$$\varphi_i(x,y) = \frac{b_2^{k_i}}{k_i!} x^{k_i} \alpha_1^{\ell_i x} \mathrm{e}^{\ell_i y}, \quad 1 \le i \le N,$$

evaluated at the N points

$$\Bigl(r_j + s_j \frac{b_1}{b_2}, \Lambda \frac{s_j}{b_2}\Bigr), \quad 1 \le j \le N.$$

To bound such a determinant, the general method consists in expanding it as a Taylor series (around the origin or any other point) of the $2N$ variables $x_j, y_j, 1 \le j \le N$, determined by the coordinates of the given N points. In our special case, the second coordinate y is small, so it appears to be sufficient to expand $\varphi_i(x, y)$ at order 1 in y. The source of the numerical improvement in [253] is precisely the use of the whole Taylor series expansion.

Proceeding as in [252] and [254], we introduce the quantity

$$\Lambda' := \Lambda \max\left\{ \frac{\mathrm{e}^{|\Lambda| LR/b_1} LR}{b_1}, \frac{\mathrm{e}^{|\Lambda| LS/b_2} LS}{b_2} \right\}.$$

Observe that

$$\log \alpha_2 = \beta \log \alpha_1 + \frac{\Lambda}{b_2}, \quad \text{with } \beta = \frac{b_1}{b_2}.$$

Since

$$\binom{r_j b_2 + s_j b_1}{k_i} = \frac{b_2^{k_i}}{k_i!} (r_j + s_j \beta)^{k_i} + (\text{terms of degree} < k_i), \quad 1 \le i, j \le n,$$

the multilinearity of the determinant implies that

$$\Delta = \det \left(\frac{b_2^{k_i}}{k_i!} (r_j + s_j \beta)^{k_i} \alpha_1{}^{\ell_i r_j} \alpha_2{}^{\ell_i s_j} \right)_{1 \le i, j \le N}.$$

Let i, j be integers with $1 \le i, j \le N$ and write

$$\alpha_1{}^{\ell_i r_j} \alpha_2{}^{\ell_i s_j} = \alpha_1{}^{\ell_i (r_j + s_j \beta)} \mathrm{e}^{\ell_i s_j \Lambda / b_2} = \alpha_1{}^{\ell_i (r_j + s_j \beta)} (1 + \Lambda' \theta_{i,j}), \tag{11.8}$$

where

$$\theta_{i,j} := \frac{\mathrm{e}^{\ell_i s_j \Lambda / b_2} - 1}{\Lambda'}$$

satisfies

$$|\theta_{i,j}| \le \frac{b_2}{LS |\Lambda| \mathrm{e}^{LS|\Lambda|/b_2}} \cdot |\mathrm{e}^{\ell_i s_j \Lambda / b_2} - 1| \le \frac{b_2}{LS |\Lambda| \mathrm{e}^{LS|\Lambda|/b_2}} \cdot (\mathrm{e}^{\ell_i s_j |\Lambda| / b_2} - 1),$$

since

$$|\mathrm{e}^u - 1| \le \mathrm{e}^{|u|} - 1, \quad \text{for every complex number } u.$$

Then, using that

$$\mathrm{e}^{\ell_i s_j |\Lambda| / b_2} - 1 \le \mathrm{e}^{LS|\Lambda|/b_2} - 1 \quad \text{and} \quad \mathrm{e}^u - 1 \le u \mathrm{e}^u, \quad \text{for } u \ge 0,$$

we deduce that

$$|\theta_{i,j}| \le 1.$$

The fact that all the $\theta_{i,j}$ are bounded by 1 in modulus explains why it is better to work with Λ' in place of Λ.

We see from (11.8) that the determinant Δ tends to 0 when Λ' tends to 0; see (11.12) below.

– *Arithmetic lower bound for* $|\Delta|$. We apply the Liouville inequality Theorem B.10 to bound $|\Delta|$ from below. Our lower bound, which involves the quantity b defined in (11.4), is slightly less precise than Lemme 6 of [254].

Lemma 11.5. *We have*

$$\log|\Delta| \geq -DN\log N - D(K-1)N\frac{\log b}{2} - DLN\bigl(Rh(\alpha_1)+Sh(\alpha_2)\bigr). \tag{11.9}$$

Proof. Consider the integer polynomial

$$P(X,Y) := \sum_{\sigma\in\mathfrak{S}_N} \operatorname{sgn}(\sigma)\prod_{i=1}^{N}\binom{r_{\sigma(i)}b_2+s_{\sigma(i)}b_1}{k_i} X^{\sum_{i=1}^{N}\ell_i r_{\sigma(i)}}Y^{\sum_{i=1}^{N}\ell_i s_{\sigma(i)}},$$

where $\operatorname{sgn}(\sigma)$ denotes the signature of the permutation σ. Using the obvious bound

$$r_jb_2+s_jb_1 \leq (R-1)b_2+(S-1)b_1, \quad j=1,\dots,N,$$

we observe that the length $\mathrm{L}(P)$ of the polynomial $P(X,Y)$ (see Definition B.9) satisfies

$$\mathrm{L}(P) \leq N!\bigl((R-1)b_2+(S-1)b_1\bigr)^{k_1+\cdots+k_N}\Bigl(\prod_{i=1}^{N}k_i!\Bigr)^{-1}.$$

Noticing that $k_1+\cdots+k_N = \frac{(K-1)N}{2}$, we get the upper bound

$$\mathrm{L}(P) \leq N^N\, b^{(K-1)N/2}, \tag{11.10}$$

with b defined in (11.4). Since, by (11.7), the degrees in X and in Y of $P(X,Y)$ do not exceed LRN and LSN, respectively, it follows from (11.10) and Theorem B.10 that

$$\log|P(\alpha_1,\alpha_2)| \geq -DN\log N - D(K-1)N\frac{\log b}{2} - DLN\bigl(Rh(\alpha_1)+Sh(\alpha_2)\bigr).$$

Since $\Delta = P(\alpha_1,\alpha_2)$, this proves the lemma. □

– *Analytic upper bound of* $|\Delta|$.

Lemma 11.6. *Let* $\rho > 1$ *be a real number. If* $|\Lambda'| \leq \rho^{-N}$, *then*

$$\begin{aligned}\log|\Delta| \leq -\frac{N(N-K)\log\rho}{2} + N\log N + \frac{KN\log b}{2}\\ + \rho LN\bigl(R|\log\alpha_1| + S|\log\alpha_2|\bigr).\end{aligned} \tag{11.11}$$

Proof. Plugging (11.8) in the expression of the determinant Δ, we get

$$\Delta = \sum_{I\subseteq\{1,\dots,N\}} (\Lambda')^{N-|I|}\Delta_I, \tag{11.12}$$

where the summation is taken over all the 2^N subsets I of $\{1, \dots, N\}$ and

$$\Delta_I := \det \begin{pmatrix} \varphi_i(z_1) & \cdots & \varphi_i(z_N) \\ & & \\ \theta_{i,1}\varphi_i(z_1) & \cdots & \theta_{i,N}\varphi_i(z_N) \end{pmatrix} \begin{array}{l} \}\ \ i \in I \\ \\ \}\ \ i \notin I \end{array} ,$$

with

$$\varphi_i(z) = b_2^{k_i} \frac{z^{k_i}}{k_i!} \alpha_1^{\ell_i z}, \quad z_j = r_j + \beta s_j, \quad 1 \le i, j \le N.$$

For a subset I of $\{1, \dots, N\}$ define the entire function Φ_I of the variable x by

$$\Phi_I(x) := \det \begin{pmatrix} \varphi_i(xz_1) & \cdots & \varphi_i(xz_N) \\ & & \\ \theta_{i,1}\varphi_i(xz_1) & \cdots & \theta_{i,N}\varphi_i(xz_N) \end{pmatrix} \begin{array}{l} \}\ \ i \in I \\ \\ \}\ \ i \notin I \end{array} \tag{11.13}$$

and observe that $\Delta_I = \Phi_I(1)$. For $i = 1, \dots, N$, let

$$\varphi_i(z) = \sum_{n \ge 0} p_{i,n} z^n$$

be the Taylor series expansion of the function φ_i. Plugging these expressions into (11.13), we obtain

$$\Phi_I(x) = \sum_{n_i : i \in I} \Big(\prod_{i \in I} p_{i,n_i} x^{n_i} \Big) \det \begin{pmatrix} z_1^{n_i} & \cdots & z_N^{n_i} \\ & & \\ \theta_{i,1}\varphi_i(xz_1) & \cdots & \theta_{i,N}\varphi_i(xz_N) \end{pmatrix} \begin{array}{l} \}\ \ i \in I \\ \\ \}\ \ i \notin I \end{array} ,$$

where the summation is taken over all the $|I|$-tuples $(n_1, \dots, n_{|I|})$ of non-negative integers. If an $|I|$-tuple is such that there are distinct indices h, k in I for which $n_h = n_k$, then the rows h and k in the determinant are equal, thus the corresponding term in the sum is zero. Consequently, the summation is taken over all the $|I|$-tuples of distinct non-negative integers. For such an $|I|$-tuple I, we have

$$\sum_{i \in I} n_i \ge 0 + \cdots + (|I| - 1) = \frac{|I|^2 - |I|}{2}.$$

Consequently, the function Φ_I has at the origin a zero of multiplicity at least $(|I|^2 - |I|)/2$. Lemma F.1 then implies that

$$|\Delta_I| = |\Phi_I(1)| \le \rho^{-(|I|^2 - |I|)/2} \max_{|x| = \rho} |\Phi_I(x)|.$$

Using this for every subset I of $\{1,\dots,N\}$ and inserting the upper bound $|\Lambda'| \le \rho^{-N}$ in (11.12), we obtain

$$\begin{aligned}|\Delta| &\le 2^N \max_{0\le i\le N} \bigl(\rho^{-N(N-i)-(i^2-i)/2}\bigr) \max_I \max_{|x|=\rho} |\Phi_I(x)| \\ &\le 2^N \rho^{-(N^2-N)/2} \max_I \max_{|x|=\rho} |\Phi_I(x)|,\end{aligned}$$

where the last but one maximum is taken over all the subsets I of $\{1,\dots,N\}$.

To bound $|\Phi_I(x)|$ from above, we expand the determinant $\Phi_I(x)$ and use that $|\theta_{i,j}| \le 1$. Then, for every complex number x of modulus ρ, we have

$$\begin{aligned}|\Phi_I(x)| \le N! \prod_{i=1}^{N} \left(\frac{(|x|((R-1)b_2+(S-1)b_1))^{k_i}}{k_i!} \right) \\ \max_\sigma \exp\left(\sum_{i=1}^{N} \ell_i (r_{\sigma(i)} + \beta s_{\sigma(i)})|x|\,|\log\alpha_1| \right) \\ \le N!\,(\rho b)^{(K-1)N/2} \exp\bigl(\rho LRN|\log\alpha_1| + \rho LSN|\log\alpha_2|\bigr),\end{aligned}$$

by (11.1), (11.7), and (11.4). Since $N\ge 6$, we get $2^N N! \le N^N$ and we obtain

$$\begin{aligned}\log|\Delta| \le -\frac{N^2\log\rho}{2} + \frac{N\log\rho}{2} + N\log N + \frac{(K-1)N\log\rho}{2} + \frac{(K-1)N\log b}{2} \\ + \rho LN\bigl(R|\log\alpha_1| + S|\log\alpha_2|\bigr).\end{aligned}$$

This completes the proof of Lemma 11.6. □

– *Completion of the proof of Theorem 11.4.* Multiplying (11.9) and (11.11) by $\frac{2}{N}$, we see that $|\Lambda'| > \rho^{-N}$ holds as soon as

$$\begin{aligned}(N-K)\log\rho > 2(D+1)\log N + (D+1)K\log b \\ + 2LR(\rho|\log\alpha_1| + D\,h(\alpha_1)) + 2LS(\rho|\log\alpha_2| + D\,h(\alpha_2)).\end{aligned}$$

This establishes Theorem 11.4.

11.4. Deduction of Theorem 11.1 from Theorem 11.4

First, we give an upper bound for the quantity b defined by (11.4).

Lemma 11.7. *For any $K\ge 2$, the quantity b satisfies*

$$b = \bigl((R-1)b_2 + (S-1)b_1\bigr)\left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)} \le 5\frac{Rb_2+Sb_1}{K-1}. \qquad (11.14)$$

Proof. For $K = 2, \dots, 7$, this is an immediate computation. Note that, for any integer $k \geq 2$, we have

$$\log k! = \sum_{j=1}^{k} \log j \geq \int_1^k \log t \,\mathrm{d}t = [t \log t - t]_1^k \geq k \log k - k$$

and

$$\sum_{j=1}^{k} j \log j \geq \int_1^k t \log t \,\mathrm{d}t \geq \frac{1}{4}[2t^2 \log t - t^2]_1^k \geq \frac{k^2}{2} \log k - \frac{k^2}{4}.$$

Thus, we have the lower bound

$$\begin{aligned}\Bigl(\prod_{k=1}^{K-1} k!\Bigr)^{\frac{2}{K^2-K}} &\geq \Bigl(\prod_{k=1}^{K-1} \mathrm{e}^{-k}\Bigr)^{\frac{2}{K^2-K}} \Bigl(\prod_{k=1}^{K-1} k^k\Bigr)^{\frac{2}{K^2-K}} \\ &\geq \mathrm{e}^{-1} \exp\Bigl(\frac{(K-1)^2 \log(K-1)}{K^2-K} - \frac{(K-1)^2}{2(K^2-K)}\Bigr) \\ &\geq \mathrm{e}^{-1}\, \mathrm{e}^{-(K-1)/(2K)}\, (K-1)^{-1/K}\, (K-1) \geq \frac{K-1}{5},\end{aligned}$$

for $K \geq 8$. This completes the proof of the lemma. □

We proceed as in [252] to choose our parameters. The parameter ρ is usually called the *radius*. It could be a priori taken very large, but in view of the terms $\rho\,|\log \alpha_1|$ and $\rho\,|\log \alpha_2|$ in the right hand side of (11.5), this inequality cannot be satisfied if ρ is too large, unless $|\log \alpha_1|$ and $|\log \alpha_2|$ happen to be simultaneously very small. This is the case when α_1 and α_2 are both very close to 1 and this will be considered separately in the next section.

By the definitions of A_1 and A_2, we get $|\log \alpha_1| \leq D \log A_1$, $|\log \alpha_2| \leq D \log A_2$, and it follows from Theorem 11.4 that $|\Lambda'| > \rho^{-N}$ holds as soon as

$$\begin{aligned}K(L-1)\log\rho > 2(D+1)\log N + (D+1)K\log b \\ + 2L(\rho+1)D(R\log A_1 + S\log A_2).\end{aligned} \tag{11.15}$$

Set $B = \max\{10, \log B'\}$, with B' defined in Section 11.1, and

$$\begin{aligned}K &= \lfloor 4900BD^3(\log A_1)(\log A_2)\rfloor, \quad L = \lfloor 4BD\rfloor, \quad R_1 = \lceil 4BD^2(\log A_2)\rceil, \\ S_1 &= \lceil 4BD^2(\log A_1)\rceil, \quad R_2 = \lceil 140BD^2(\log A_2)\rceil, \quad S_2 = \lceil 140BD^2(\log A_1)\rceil.\end{aligned}$$

Note that, by (11.4),

$$\begin{aligned}\log b &\leq \log 5 + \log\Bigl(\frac{(R_1+R_2)b_2 + (S_1+S_2)b_1}{K-1}\Bigr) \\ &\leq \log\Bigl(\frac{b_2}{D\log A_1} + \frac{b_1}{D\log A_2}\Bigr) \leq B.\end{aligned} \tag{11.16}$$

Observe that $R_1 \geq L$ and $S_1 \geq L$, since we have assumed $D \log A_1 \geq 1$ and $D \log A_2 \geq 1$. Thus, if α_1 and α_2 are not both roots of unity (in which case the proof of the theorem follows straightforwardly from Theorem B.10), then condition (11.2) is satisfied. Observe also that $R_2 S_2 > (K-1)L$. Consequently, if we furthermore assume that all the elements of the set

$$\{rb_2 + sb_1 : 0 \leq r < R_2,\, 0 \leq s < S_2\}$$

are distinct, then condition (11.3) is satisfied.

We check that (11.15) is satisfied with the choice $\rho = 3$. Thus, Theorem 11.4 implies the lower bound

$$\log |\Lambda'| \geq -N \log \rho \geq -21550\, D^4 (\log A_1)(\log A_2) B^2.$$

By the definition of Λ' and the crude upper bound

$$1 + \log L + \log R + \log S \leq D^4 (\log A_1)(\log A_2) B^2,$$

we conclude that

$$\log |\Lambda| \geq -21600\, D^4 (\log A_1)(\log A_2) B^2, \tag{11.17}$$

provided that (11.3) is satisfied.

It remains for us to consider the case where (11.3) is not satisfied. Assume that there exist integers r and s such that $|r| \leq R-1$, $|s| \leq S-1$ and $rb_2 + sb_1 = 0$. We then have

$$|\Lambda| = \frac{b_1}{r} \, |s \log \alpha_2 + r \log \alpha_1|. \tag{11.18}$$

It follows from Theorem B.10 that

$$|\alpha_1^r \alpha_2^s - 1| \geq -D\big(\log 2 + Rh(\alpha_1) + Sh(\alpha_2)\big),$$

which, combined with (11.18), implies a lower bound sharper than (11.17). This concludes the proof of the theorem. □

11.5. Deduction of Theorem 11.2 from Theorem 11.4

We assume that α_1 and α_2 are real numbers greater than 1. We have established at the end of Section 11.3 that $|\Lambda'| > \rho^{-N}$ holds as soon as

$$\begin{aligned} K(L-1) \log \rho \geq{} & 2(D+1) \log N + (D+1) K \log b \\ & + 2LR(\rho \log \alpha_1 + D\, h(\alpha_1)) + 2LS(\rho \log \alpha_2 + D\, h(\alpha_2)). \end{aligned} \tag{11.19}$$

To derive (11.15) in the previous section, we have bounded $D\, h(\alpha_j)$ and $\log \alpha_j$ by $D \log A_j$, for $j = 1, 2$. This is far from being sharp when $\log \alpha_j$ is very small compared to $D\, h(\alpha_j)$, in which case the radius ρ can be chosen quite large.

We introduce a new parameter E defined by

$$E = 1 + \min \left\{ \frac{D \log A_1}{\log \alpha_1}, \frac{D \log A_2}{\log \alpha_2} \right\},$$

and, using the inequality $\log \alpha_j \le D \log A_j$, for $j = 1, 2$, we check that

$$E \log \alpha_1 \le 2D \log A_1, \quad E \log \alpha_2 \le 2D \log A_2.$$

We assume that

$$E \le \min\{A_1^{3D/2}, A_2^{3D/2}\}. \tag{11.20}$$

With $\rho = E$, the condition (11.19) is satisfied if

$$K(L-1) > \frac{2D}{\log \rho} \big(2 \log N + K \log b + 3L(R \log A_1 + S \log A_2)\big),$$

since $D + 1 \le 2D$.

Then, we choose

$$B = \max\Big\{3 \frac{\log \rho}{D}, \log B'\Big\} \tag{11.21}$$

and, since $\log b \le B$, Inequality (11.19) is satisfied if

$$K(L-1) > \frac{2D}{\log \rho} \big(2 \log N + KB + 3L(R \log A_1 + S \log A_2)\big). \tag{11.22}$$

Set

$$D^* = \frac{D}{\log \rho}$$

and observe that, by (11.20) and (11.21), we have

$$D^* \min\{\log A_1, \log A_2\} \ge \frac{2}{3}, \quad D^* B \ge 3.$$

Set

$$\begin{aligned} K &= \lfloor 4900 B (D^*)^3 (\log A_1)(\log A_2) \rfloor, \quad L = \lfloor 16 B D^* \rfloor, \\ R_1 &= \lceil 32 B (D^*)^2 (\log A_2) \rceil, \quad S_1 = \lceil 32 B (D^*)^2 (\log A_1) \rceil, \\ R_2 &= \lceil 280 B (D^*)^2 (\log A_2) \rceil, \quad S_2 = \lceil 280 B (D^*)^2 (\log A_1) \rceil. \end{aligned}$$

We check that (11.22) is satisfied. Consequently, Theorem 11.4 implies the lower bound

$$\log |\Lambda'| \ge -N \log \rho \ge -78450 (D^*)^4 (\log A_1)(\log A_2) B^2 (\log \rho).$$

By the definition of Λ' and the crude upper bound

$$1 + \log L + \log R + \log S \le (D^*)^4 (\log A_1)(\log A_2) B^2 (\log \rho),$$

we conclude that

$$\log |\Lambda| \ge -78500 D^4 (\log A_1)(\log A_2) \Big(\max\Big\{3 \frac{\log \rho}{D}, \log B'\Big\}\Big)^2 (\log \rho)^{-3},$$

provided that (11.3) is satisfied. We argue as at the end of Section 11.4 if (11.3) is not satisfied. This ends the proof of Theorem 11.2. □

Chapter 12
Lower bounds for linear forms in two p-adic logarithms: proofs

The purpose of this chapter is to present complete proofs of versions of Theorems 2.12 and 2.13, with the same dependence in all the parameters, but with larger numerical constants. Not to focus on the size of these constants allows some simplification in the proofs.

12.1. Three estimates for linear forms in two p-adic logarithms

Let p be a prime number and α_1 and α_2 complex algebraic numbers. Let $\mathfrak{p}$ be a prime ideal of the ring of integers of $\mathbb{Q}(\alpha_1, \alpha_2)$ lying above p. We denote by v_p the p-adic valuation on $\mathbb{Q}(\alpha_1, \alpha_2)$ induced by $\mathrm{v}_{\mathfrak{p}}$ and which extends the p-adic valuation v_p on $\mathbb{Q}$ normalized such that $\mathrm{v}_p(p) = 1$.

The next theorem gives an upper bound for the p-adic valuation of the difference between integral powers of α_1 and α_2. It is a corollary to the main result of [129]. As noted below Theorem 2.12, the assumption $\mathrm{v}_p(\alpha_1) = \mathrm{v}_p(\alpha_2) = 0$ is not restrictive.

Theorem 12.1. *Let p be a prime number. Let α_1 and α_2 be multiplicatively independent complex algebraic numbers with $\mathrm{v}_p(\alpha_1) = \mathrm{v}_p(\alpha_2) = 0$. Set $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$. Let A_1 and A_2 be real numbers with*

$$\log A_1 \geq \max\Big\{h(\alpha_1), \frac{1}{D}\Big\}, \quad \log A_2 \geq \max\Big\{h(\alpha_2), \frac{1}{D}\Big\}.$$

Let b_1, b_2 be non-zero integers and set

$$B' = \frac{|b_1|}{D \log A_2} + \frac{|b_2|}{D \log A_1}.$$

Then, we have the upper bound

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \leq 132000 \, \frac{p^D - 1}{(\log p)^4} D^4 \log A_1 \log A_2 \Big(\max\Big\{\log B' + \log\log p, \frac{10 \log p}{D}\Big\}\Big)^2.$$

As in Theorem 11.1, the factor $\log B'$ occurs with an exponent two: this is a consequence of the method.

Unlike in Theorem 2.3, we do not assume in Theorem 12.1 that $\log A_1$ and $\log A_2$ exceed $\frac{\log p}{D}$, but only that they exceed $\frac{1}{D}$. This refinement, which was first noticed by Yamada [442], allows us to deduce Theorem 12.3 below directly from Theorem 12.1.

Theorem 12.2 below refines Theorem 12.1 in the special case where α_1 and α_2 are multiplicatively independent non-zero rational numbers which are p-adically close to 1. It involves an extra parameter E, which plays a similar rôle as the parameter also called E in Theorem 11.2.

Theorem 12.2. *Let $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ be non-zero multiplicatively independent rational numbers. Let b_1 and b_2 be non-zero integers. Let p be a prime number. Assume that there exist a positive integer g and a real number $E \geq 3$ such that*

$$\mathrm{v}_p\Big(\Big(\frac{x_1}{y_1}\Big)^g - 1\Big) \geq E$$

and at least one of the two following conditions

$$\mathrm{v}_p\Big(\Big(\frac{x_2}{y_2}\Big)^g - 1\Big) \geq E$$

or

$$\mathrm{v}_p\Big(\Big(\frac{x_2}{y_2}\Big)^g - 1\Big) \geq 1 \quad \textit{and} \quad \mathrm{v}_p(b_2) \leq \mathrm{v}_p(b_1)$$

is satisfied. Let A_1, A_2 be real numbers with

$$\log A_j \geq \max\{\log |x_j|, \log |y_j|, E \log p\}, \qquad j = 1, 2,$$

and put

$$B' = \frac{|b_1|}{\log A_2} + \frac{|b_2|}{\log A_1}.$$

Then we have the upper estimate

$$\mathrm{v}_p\Big(\Big(\frac{x_1}{y_1}\Big)^{b_1} - \Big(\frac{x_2}{y_2}\Big)^{b_2}\Big) \leq 88000 \frac{g}{E^3 (\log p)^4} \log A_1 \log A_2 \\ \big(\max\{\log\log p + \log B', 10E \log p\}\big)^2.$$

We display an important consequence of Theorem 12.1, which is a key ingredient in the proof of a conjecture of Erdős given in Chapter 7.

Theorem 12.3. *Let p be an odd prime number and a, b integers with $a > b \geq 1$. If p does not divide ab, then*

$$\mathrm{v}_p(a^{p-1} - b^{p-1}) \leq 132 \cdot 10^5 \frac{p}{(\log p)^2} (\log 5a)(\log 5b).$$

A similar result was first established by Yamada [442] by means of a slight modification of the choice of the auxiliary parameters in [129]. Theorem 12.3 is proved in Section 12.6.

12.2. Two auxiliary inequalities involving several parameters

Keep the notation and assumption of Theorem 12.1. Assume also that b_1 and b_2 are positive. This is not at all restrictive since α_1 and α_2 are p-adic units and the height of a non-zero algebraic number is equal to the height of its inverse. Our results depend among other things on several parameters related to α_1, α_2, and $\mathfrak{p}$. We denote by e the ramification index of $\mathfrak{p}$ and by t the non-negative integer satisfying the inequalities

$$p^{t-1} \le \frac{3e}{2(p-1)} < p^t. \tag{12.1}$$

Put $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}|$. Let Ψ denote the isomorphism between the completion of $\mathbb{Q}(\alpha_1, \alpha_2)$ with respect to $\mathfrak{p}$ and a sub-field of $\mathbb{C}_p$, which we write $\mathbb{Q}_p(\alpha_1, \alpha_2)$. Then, we have $\mathrm{v}_p(\alpha) = \mathrm{v}_p(\Psi(\alpha))$ for every non-zero α in $\mathbb{Q}(\alpha_1, \alpha_2)$; see Section B.1.

Let g denote the smallest positive integer such that

$$\mathrm{v}_p(\alpha_1^g - 1) > 0 \quad \text{and} \quad \mathrm{v}_p(\alpha_2^g - 1) > 0.$$

The assumption $\mathrm{v}_p(\alpha_1) = \mathrm{v}_p(\alpha_2) = 0$ ensures that g exists. We recall that g divides $p^D - 1$ (actually, g divides $p^f - 1$, where f is the residue degree of $\mathfrak{p}$; see Lemma F.4). We fix a g-th primitive root ζ of unity in $\overline{\mathbb{Q}}_p$. Let m_1, m_2 be integers such that, defining θ_1 and θ_2 by

$$\alpha_1 = \zeta^{m_1}\, \theta_1 \quad \text{and} \quad \alpha_2 = \zeta^{m_2}\, \theta_2,$$

we have $\mathrm{v}_p(\theta_1 - 1) = \mathrm{v}_p(\alpha_1^g - 1) > 0$ and $\mathrm{v}_p(\theta_2 - 1) = \mathrm{v}_p(\alpha_2^g - 1) > 0$. By Lemma F.3, the choice of t ensures that

$$\mathrm{v}_p(\theta_1^{p^t} - 1) > \frac{1}{p-1}, \quad \mathrm{v}_p(\theta_2^{p^t} - 1) > \frac{1}{p-1}.$$

The main result of [129] is the following.

Theorem 12.4. *Let $K \ge 3$, L, R_1, R_2, S_1, S_2 be integers at least equal to 2. Set $R = R_1 + R_2 - 1$, $S = S_1 + S_2 - 1$, and $N = KL$. Set*

$$b = \big((R-1)b_2 + (S-1)b_1\big)\Bigg(\prod_{k=1}^{K-1} k!\Bigg)^{-2/(K^2-K)}.$$

Let t be defined by (12.1). Assume that there are two residue classes c_1 and c_2 modulo g such that

$$\begin{aligned} \mathrm{Card}\big\{\alpha_1^{p^t r}\, \alpha_2^{p^t s} : 0 \le r < R_1,\ 0 \le s < S_1,\ m_1 r + m_2 s \equiv c_1 \text{ modulo } g\big\} &\ge L, \\ \mathrm{Card}\big\{r b_2 + s b_1 : 0 \le r < R_2,\ 0 \le s < S_2,\ m_1 r + m_2 s \equiv c_2 \text{ modulo } g\big\} &> (K-1)L. \end{aligned} \tag{12.2}$$

Assume furthermore that

$$(N-K)(\log p) > 3D\,\big(2\log N + (K-1)\log b + LRh(\alpha_1) + LSh(\alpha_2)\big). \tag{12.3}$$

Denoting by p^u the greatest power of p which divides simultaneously b_1 and b_2, we have

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \le 2KL + u.$$

The next theorem is a variant of Theorem 12.4 and a version of it was established in [109]. It is of interest in the particular case where α_1^g and α_2^g are p-adically very close to one.

Theorem 12.5. *Let K, L, R_1, R_2, S_1, S_2, R, S, N, and b be as in the statement of Theorem 12.4. Assume that there exist two residue classes c_1 and c_2 modulo g such that (12.2) holds, where t is defined by (12.1). Denote by p^u the greatest power of p which divides simultaneously b_1 and b_2. Assume furthermore that there exists a real number E such that*

$$\mathrm{v}_p(\alpha_1^g - 1) \geq E > 1 + \frac{1}{p-1}$$

and that either

$$\mathrm{v}_p(\alpha_2^g - 1) \geq E > 1 + \frac{1}{p-1},$$

or

$$\mathrm{v}_p(\alpha_2^g - 1) > 0 \quad \text{and } p \text{ does not divide } \frac{b_2}{p^u}.$$

Under the condition

$$(N-K)(E+t-1)(\log p) > D\big(2\log N + (K-1)\log b + 2LRp^t h(\alpha_1) + 2LSp^t h(\alpha_2)\big),$$

we have

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) < (E+t)KL + u.$$

If α_1 and α_2 are rational numbers, then the condition

$$(N-K)(E-1)(\log p) > 2\log N + (K-1)\log b + 4LR\,h(\alpha_1) + 4LS\,h(\alpha_2)$$

implies that

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) < (E+1)KL + u.$$

Our assumption on E in Theorem 12.5 is slightly stronger than in [109]. This is due to the fact that we do not use the Schur polynomials as in [129]. The quantity E is analogous to the parameter $\log\rho$ in Chapter 11.

In comparison with the complex case, an extra difficulty in the p-adic setting is caused by the fact that the radius of convergence of the p-adic exponential function is $p^{-1/(p-1)}$, thus it is not infinite as for the complex exponential function. Consequently, to be able to apply p-adic analysis, we have first to find some trick in order to place us within the disc of convergence of the p-adic exponential function. A naïve answer consists in working with $\mathrm{v}_p(\alpha_1^g - \alpha_2^g)$ instead of $\mathrm{v}_p(\alpha_1 - \alpha_2)$, in which case no congruence conditions would be needed in (12.2), but α_1 and α_2 would have to be replaced by their g-th power in (12.3). Consequently, we would have a factor $gL(Rh(\alpha_1) + Sh(\alpha_2))$ and, ultimately, an upper bound for $\mathrm{v}_p(\alpha_1 - \alpha_2)$ involving g^2 and not g (since g divides $p^D - 1$, we would get eventually a bound involving $(p^D - 1)^2$). A more clever way to proceed consists in working with $\mathrm{v}_p(\theta_1 - \theta_2)$, since θ_1 and θ_2 are principal units. The price to pay is then the congruence conditions occurring in (12.2), which impose the inequalities $R_1 S_1 \geq gL$ and $R_2 S_2 > g(K-1)L$ and, ultimately, cost (only) a factor g. This explains the presence of the factor $p^D - 1$ in Theorem 12.1.

To remove this factor for abitrary α_1 and α_2, or to replace it by a quantity significantly smaller, remains a major open problem. However, the preceding discussion shows that the factor $p^D - 1$ can indeed be removed when α_1 and α_2 are both principal units (that is, if $g = 1$). If, moreover, these algebraic numbers are p-adically very close to 1, then the functions $z \mapsto \alpha_1^z$ and $z \mapsto \alpha_2^z$ are analytic on a large disc (see Lemma F.7) and we can take advantage of this to improve the conclusion of Theorem 12.1 in this particular case: this is precisely the purpose of Theorem 12.2.

12.3. Proofs of Theorems 12.4 and 12.5

We keep the notation of Section 12.2 and assume that all the hypotheses of Theorem 12.4 until (12.2) are satisfied.

Our proof is very close to that of Theorem 11.3 and, at one step, it differs from the proof in [129], where the authors used Schur polynomials instead of the Schwarz lemma to obtain the analytic estimate. We have decided not to include this improvement, which is however crucial for obtaining very good numerical constants. For this reason, we had to define the quantity t in a slightly different way as in [129].

Observe that $RS > KL$. By Lemma E.1 applied with

$$\mathcal{E} = \big\{(r,s) : 0 \leq r < R_1,\ 0 \leq s < S_1,\ m_1 r + m_2 s \equiv c_1 \text{ modulo } g\big\}$$

and

$$\mathcal{E}' = \big\{(r',s') : 0 \leq r' < R_2,\ 0 \leq s' < S_2,\ m_1 r' + m_2 s' \equiv c_2 \text{ modulo } g\big\},$$

the $KL \times RS$ matrix $\mathcal{M}$ whose coefficients are the complex numbers

$$\binom{rb_2 + sb_1}{k} {\alpha_1}^{p^t \ell r} {\alpha_2}^{p^t \ell s}$$

is of maximal rank, equal to $N = KL$. To see this, observe that if the KL lines of $\mathcal{M}$ were linearly dependent, then there would exist a non-zero integer polynomial $P(X,Y)$, whose degree in X is at most $K-1$ and whose degree in Y is at most $L-1$, vanishing at all the points $(rb_2 + sb_1, \alpha_1^{p^t r} \alpha_2^{p^t s})$ with $0 \leq r < R$, $0 \leq s < S$. This would contradict Lemma E.1.

We can thus extract from $\mathcal{M}$ a non-zero minor Δ of size $N \times N$, which can be written, with a suitably ordering of the columns,

$$\Delta = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} {\alpha_1}^{p^t \ell_i r_j} {\alpha_2}^{p^t \ell_i s_j} \right)_{1 \leq i,j \leq N}.$$

We index the lines by pairs (k,ℓ) and the columns by pairs (r,s). For convenience, we fix the numbering using the formulas

$$k_i = i - 1 - K\lfloor (i-1)/K \rfloor, \quad \ell_i = \lfloor (i-1)/K \rfloor, \quad \text{for } i = 1, \ldots, KL.$$

The columns are indexed by the N distinct pairs of integers $(r_1, s_1), \dots, (r_N, s_N)$, where $0 \le r_j < R$ and $0 \le s_j < S$ for $j = 1, \dots, N$. In the sequel, we will use repeatedly that, for any permutation σ of the set $\{1, \dots, N\}$ we have

$$\sum_{i=1}^{N} \ell_i r_{\sigma(i)} \le LRN \quad \text{and} \quad \sum_{i=1}^{N} \ell_i s_{\sigma(i)} \le LSN. \tag{12.4}$$

The strategy of the proof goes as follows. By construction, we know that Δ is non-zero. We bound $\mathrm{v}_p(\Delta)$ from above by means of Liouville's inequality Theorem B.10 and from below by using p-adic analysis, namely the p-adic maximum principle. Then, we show that the lower bound exceeds the upper bound if $\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2})$ is large enough. This contradiction implies that $\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2})$ cannot be too large.

We establish Theorems 12.4 and 12.5 simultaneously. In view of their assumptions, we can suppose without any loss of generality that p does not divide b_2/p^u.

– *Arithmetic upper bound for* $\mathrm{v}_p(\Delta)$. We have the following analogue of Lemma 11.5.

Lemma 12.6. *We have the upper bound*

$$\mathrm{v}_p(\Delta) \le \frac{DN}{2e(\log p)} \Big(2 \log N + (K-1) \log b + 2p^t L\big(Rh(\alpha_1) + Sh(\alpha_2)\big)\Big).$$

Proof. This is a variant of Lemma 11.5. Consider the polynomial

$$P(X, Y) = \sum_{\sigma \in \mathfrak{S}_N} \mathrm{sgn}(\sigma) \prod_{i=1}^{N} \binom{r_{\sigma(i)} b_2 + s_{\sigma(i)} b_1}{k_i} X^{\sum_{i=1}^{N} \ell_i r_{\sigma(i)}} Y^{\sum_{i=1}^{N} \ell_i s_{\sigma(i)}},$$

where $\mathrm{sgn}(\sigma)$ denotes the signature of the permutation σ. Since, by (12.4), the degrees in X and in Y of $P(X, Y)$ do not exceed LRN and LSN, respectively, it follows from (11.10) and Theorem B.10 that

$$\log |P(\alpha_1^{p^t}, \alpha_2^{p^t})|_v \ge -\frac{D}{e} \Big(N \log N + (K-1)N \frac{\log b}{2} + p^t NL\big(Rh(\alpha_1) + Sh(\alpha_2)\big)\Big),$$

where $|\cdot|_v$ is the absolute value associated with $\mathfrak{p}$ and e is the ramification index of $\mathfrak{p}$. This completes the proof of the lemma, since $\Delta = P(\alpha_1^{p^t}, \alpha_2^{p^t})$ and $\log |\Delta|_v = -\mathrm{v}_p(\Delta) \log p$, by (B.3). □

– *Analytic lower bound for* $\mathrm{v}_p(\Delta)$. There is an extra difficulty when b_1 and b_2 are both divisible by p. We introduce a quantity E^* to deal simultaneously with the proofs of Theorems 12.4 and 12.5. For the proof of Theorem 12.4 we set $E^* = \frac{p^t}{3e} + \frac{1}{p-1}$, while we set $E^* = E + t$ with $E > 1 + \frac{1}{p-1}$ in the proof of Theorem 12.5. In both cases, we have $E^* > \frac{1}{p-1}$.

Lemma 12.7. *Assume that*

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \ge E^* N + u.$$

Then,

$$\mathrm{v}_p(\Delta) \ge \Big(E^* - \frac{1}{p-1}\Big) \frac{N(N-K)}{2}.$$

Proof. Assume first that $u \geq 1$. Some extra arguments are needed in this case. Since

$$m_1 r_j + m_2 s_j \equiv c_1 + c_2 \bmod g, \quad j = 1, \dots, N,$$

and $\alpha_1 = \zeta^{m_1}\theta_1, \alpha_2 = \zeta^{m_2}\theta_2$, we get

$$\Delta = \zeta^{(c_1+c_2)p^t(\ell_1+\dots+\ell_N)}\Delta',$$

where

$$\Delta' = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} {\theta_1}^{p^t \ell_i r_j} {\theta_2}^{p^t \ell_i s_j}\right)_{1 \leq i,j \leq N}.$$

In particular, we have $\mathrm{v}_p(\Delta) = \mathrm{v}_p(\Delta')$. Furthermore, since the p-adic valuation of

$$\Lambda := \alpha_1^{b_1} - \alpha_2^{b_2} = \zeta^{m_1 b_1}\theta_1^{b_1} - \zeta^{m_2 b_2}\theta_2^{b_2}$$

is positive, the integers $m_1 b_1$ and $m_2 b_2$ are in the same class modulo g. Setting

$$\widetilde{\Lambda} = \theta_1^{b_1} - \theta_2^{b_2},$$

we have $\mathrm{v}_p(\Lambda) = \mathrm{v}_p(\widetilde{\Lambda})$. Define the quantities

$$b_1' = \frac{b_1}{p^u}\,,\; b_2' = \frac{b_2}{p^u}\,,\; \sigma = \frac{\theta_1^{b_1'}}{\theta_2^{b_2'}}.$$

Observe that

$$\mathrm{v}_p\big(\sigma^{p^u} - 1\big) = \mathrm{v}_p\Big(\frac{\widetilde{\Lambda}}{\theta_2^{b_2}}\Big) = \mathrm{v}_p(\Lambda) \geq E^* N + u > \frac{1}{p-1} + u,$$

by assumption, thus

$$\sum_{\xi} \mathrm{v}_p(\sigma - \xi) = \mathrm{v}_p(\Lambda) \geq E^* N + u > \frac{1}{p-1} + u,$$

where the sum is taken over all the p^u-th roots of unity ξ in $\overline{\mathbb{Q}}_p$.

We then show that σ is near one, and exactly one, of these roots. Order the p^u-th roots of unity $\xi_1, \dots, \xi_{p^u}$ in such a way that

$$\mathrm{v}_p(\sigma - \xi_1) \geq \cdots \geq \mathrm{v}_p(\sigma - \xi_{p^u}).$$

It follows that

$$\mathrm{v}_p\Big(\frac{\xi_j}{\xi_1} - 1\Big) = \mathrm{v}_p(\xi_j - \xi_1) \geq \mathrm{v}_p(\sigma - \xi_j), \quad j = 2, \dots, p^u.$$

Thus,

$$\mathrm{v}_p(\sigma - \xi_1) + \sum_{\substack{\xi^{p^u}=1 \\ \xi \neq 1}} \mathrm{v}_p(\xi - 1) \geq E^* N + u > \frac{1}{p-1} + u. \tag{12.5}$$

It follows from Lemma F.5 that the sum in (12.5) is equal to u. This gives $\mathrm{v}_p(\sigma-\xi_1) > \frac{1}{p-1}$. If $\mathrm{v}_p(\sigma-\xi_1) = \mathrm{v}_p(\sigma-\xi_2)$, then, by the first assertion of Lemma F.5, we have

$$\frac{1}{p^{w-1}(p-1)} = \mathrm{v}_p\Big(\frac{\xi_2}{\xi_1}-1\Big) = \mathrm{v}_p(\xi_2-\xi_1) > \frac{1}{p-1},$$

where p^w denotes the exact order of the root of unity $\frac{\xi_2}{\xi_1}$. Since $\xi_1 \neq \xi_2$, we have $w \geq 1$. We get a contradiction and conclude that $\mathrm{v}_p(\sigma-\xi_1) > \mathrm{v}_p(\sigma-\xi_j)$ holds for $j = 2, \dots, p^u$.

Lemma F.6 then shows that ξ_1 belongs to the field $\mathbb{Q}_p(\sigma)$. Assume that $\xi_1 \neq 1$ and denote by p^w its order. Then, we have

$$p^{w-1}(p-1) \leq e < \frac{2}{3}p^t(p-1),$$

since, by Lemma F.5, the ramification index of the extension $\mathbb{Q}_p(\xi_1)/\mathbb{Q}_p$ is equal to $p^{w-1}(p-1)$. We derive that $p^w \leq p^t$, thus $\xi_1^{p^t} = 1$, which is obviously true also when $\xi_1 = 1$. Set

$$\Lambda' = \theta_1^{b_1'} - \xi_1\theta_2^{b_2'}.$$

Since ξ_1 is a p^u-th root of unity and $\mathrm{v}_p(\sigma-\xi_1) > \frac{1}{p-1}$, Lemma F.2 implies that

$$\begin{aligned}\mathrm{v}_p(\Lambda) = \mathrm{v}_p(\widetilde{\Lambda}) = \mathrm{v}_p\big(\sigma^{p^u}-1\big) &= \mathrm{v}_p\Big(\Big(\frac{\sigma}{\xi_1}\Big)^{p^u}-1\Big)\\ &= \mathrm{v}_p(\sigma-\xi_1)+u = \mathrm{v}_p(\Lambda')+u.\end{aligned}$$

We then get the lower bound

$$\mathrm{v}_p(\Lambda') \geq \mathrm{v}_p(\Lambda) - u \geq E^*N.$$

This also holds when $u = 0$ by setting $\Lambda' = \widetilde{\Lambda}$ and $\xi_1 = 1$.

Recall that p does not divide b_2'. Set $\beta = \frac{b_1}{b_2} = \frac{b_1'}{b_2'}$ and write

$$\theta_2^{b_2'} = \frac{\theta_1^{b_1'} - \Lambda'}{\xi_1} = \frac{\theta_1^{b_1'}(1-\theta_1^{-b_1'}\Lambda')}{\xi_1}.$$

Let $i = 1, \dots, N$ and $j = 1, \dots, N$. Since $\mathrm{v}_p(b_2') = 0$ and $\xi_1^{p^t} = 1$, we get

$$\begin{aligned}\theta_2^{p^t\ell_is_j} &= (\theta_1^{p^t})^{\beta\ell_is_j}(1-\theta_1^{-b_1'}\Lambda')^{p^t\ell_is_j/b_2'}\\ &= (\theta_1^{p^t})^{\beta\ell_is_j}(1+\sigma_{i,j}\Lambda'),\end{aligned}$$

where $\sigma_{i,j}$ is in $\overline{\mathbb{Q}}_p$. All these expressions are well-defined since the p-adic valuations of β and p^t/b_2 are non-negative and $\theta_1^{p^t}-1$ and $\theta_1^{-b_1'}\Lambda'$ are in the disc of convergence of the p-adic exponential function; see Section F.3. Furthermore, since $\mathrm{v}_p(\ell_is_j/b_2') \geq 0$, we deduce that $|\sigma_{i,j}|_p \leq 1$.

We can now substitute the above expressions in the determinant Δ'. By multilinearity of the determinant, we get

$$\begin{aligned}\Delta' &= \det\left(\frac{(r_jb_2+s_jb_1)^{k_i}}{k_i!}\theta_1^{p^t\ell_i(r_j+s_j\beta)}(1+\sigma_{i,j}\Lambda')\right)_{1\le i,j\le N}\\ &= b_2^{k_1+\cdots+k_N}\det\left(\frac{(r_j+s_j\beta)^{k_i}}{k_i!}\theta_1^{p^t\ell_i(r_j+s_j\beta)}(1+\sigma_{i,j}\Lambda')\right)_{1\le i,j\le N}\\ &= b_2^{N(K-1)/2}\Bigg(\sum_{I\subseteq\{1,\dots,N\}}(\Lambda')^{N-|I|}\Delta'_I\Bigg),\end{aligned}\tag{12.6}$$

where, for every subset I of $\{1,\dots,N\}$, we have written

$$\Delta'_I = \det\begin{pmatrix}\varphi_i(z_1) & ,\dots, & \varphi_i(z_N)\\ \\ \sigma_{i,1}\varphi_i(z_1) & ,\dots, & \sigma_{i,N}\varphi_i(z_N)\end{pmatrix}\begin{matrix}\}\quad i\in I\\ \\ \}\quad i\notin I\end{matrix}$$

with

$$\varphi_i(z)=\frac{z^{k_i}}{k_i!}\theta_1^{p^t\ell_i z},\quad z_j=r_j+\beta s_j,\quad 1\le i,j\le N.$$

It follows from Lemmas F.3 (for $E^*=\frac{p^t}{3e}$) and F.2 (for $E^*=E+t$) that $\mathrm{v}_p(\theta_1^{p^t}-1)\ge E^*$. Since $E^*>\frac{1}{p-1}$, we infer from Lemma F.7 that, for $i=1,\dots,N$, the function φ_i is analytic for z with $\mathrm{v}_p(z)\ge -E^*+\frac{1}{p-1}$.

Unlike in [129], we do not use here the Schur determinants, which would yield a better numerical estimate. We keep the same steps as in the proof of Theorem 11.3 and apply the p-adic Schwarz lemma.

Let I be a subset of $\{1,\dots,N\}$. Consider the function Φ_I of the variable x defined for x in $\mathbb{C}_p$ with $\mathrm{v}_p(x)\ge -E^*+\frac{1}{p-1}$ by

$$\Phi_I(x) := \det\begin{pmatrix}\varphi_i(xz_1) & ,\dots, & \varphi_i(xz_N)\\ \\ \sigma_{i,1}\varphi_i(xz_1) & ,\dots, & \sigma_{i,N}\varphi_i(xz_N)\end{pmatrix}\begin{matrix}\}\quad i\in I\\ \\ \}\quad i\notin I\end{matrix}$$

in such a way that $\Delta'_I=\Phi_I(1)$. Expanding in Taylor series the functions φ_i for the indices i in I, we argue as in Section 11.3 to see that the function Φ_I has at the point $x=0$ a zero of multiplicity at least $(|I|^2-|I|)/2$, where $|I|$ is the cardinality of I.

Set

$$\rho = p^{E^*-1/(p-1)}.\tag{12.7}$$

Since the function Φ_I is analytic on $\{z : |z|_p\le\rho\}$, we deduce from Lemma F.8 that

$$|\Delta_I|_p = |\Phi_I(1)|_p \le \rho^{-(|I|^2-|I|)/2}\max_{|x|_p=\rho}|\Phi_I(x)|_p.$$

Using this for every subset I of $\{1,\dots,N\}$ and inserting the upper bound

$$|\Lambda'|_p \le p^{-E^*N} \le \rho^{-N}$$

in (12.6), we obtain by means of the ultrametric inequality that

$$\begin{aligned}|\Delta'|_p &\le \max_{1\le i\le N} \bigl(\rho^{-N(N-i)-(i^2-i)/2}\bigr) \max_I \max_{|x|_p=\rho} |\Phi_I(x)|_p \\ &\le \rho^{-(N^2-N)/2} \max_I \max_{|x|_p=\rho} |\Phi_I(x)|_p,\end{aligned} \tag{12.8}$$

where the last but one maximum is taken over all the subsets I of $\{1,\dots,N\}$. It remains for us to bound $|\Phi_I(x)|_p$ from above. To this end, we expand the determinant $\Phi_I(x)$ and we use that $|\sigma_{i,j}|_p \le 1$, for $1\le i,j\le N$. Then, for every x with $|x|_p\le\rho$, the ultrametric inequality implies that

$$|\Phi_I(x)|_p \le \rho^{-(k_1+\dots+k_N)} = \rho^{-N(K-1)/2},$$

hence, by (12.8),

$$|\Delta|_p = |\Delta'|_p \le \rho^{-(N^2-N+NK+N)/2} = \rho^{-N(N-K)/2}.$$

We conclude from (12.7) that

$$\mathrm{v}_p(\Delta) \ge \Bigl(E^* - \frac{1}{p-1}\Bigr)\frac{N(N-K)}{2}.$$

This completes the proof of the lemma. □

– *Choice of the parameters.* We first deal with Theorem 12.4, in which case $E^* - \frac{1}{p-1} = \frac{p^t}{3e}$. It then follows from Lemmas 12.6 and 12.7 that the assumption

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \ge E^*N + u$$

yields a contradiction as soon as

$$\frac{p^t}{3e}(N-K) > \frac{D}{e(\log p)}\bigl(2\log N + (K-1)\log b + 2p^tL\bigl(Rh(\alpha_1)+Sh(\alpha_2)\bigr)\bigr).$$

Consequently, under the assumptions of Theorem 12.4, the inequality

$$(N-K) \ge \frac{3D}{\log p}\bigl(2\log N + (K-1)\log b + 2L\bigl(R\log A_1 + S\log A_2\bigr)\bigr)$$

implies

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) < 2N + u,$$

since $E^* \le 2$. This establishes Theorem 12.4.

Likewise, using that $E^* = E + t$ in the setting of Theorem 12.5, it follows from Lemmas 12.6 and 12.7 that the assumption

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \geq E^* N + u$$

yields a contradiction as soon as

$$(E + t - 1)(N - K) > \frac{D}{e(\log p)} \big(2 \log N + (K-1) \log b + 2p^t L\big(Rh(\alpha_1) + Sh(\alpha_2)\big)\big).$$

In the special case where α_1 and α_2 are rational numbers, we have $e = D = 1$. Furthermore, $t = 0$ if $p \geq 3$ and $t = 1$ if $p = 2$. We crudely bound $E + t - 1$ from below by $E - 1$ and p^t from above by 2. This completes the proof of Theorem 12.5.

12.4. Deduction of Theorem 12.1 from Theorem 12.4

We proceed essentially as in the proof of Theorem 11.1 to choose the parameters. Define

$$D^* = \frac{D}{\log p} \quad \text{and} \quad g^* = \max\{g, (\log p)^2\}.$$

The introduction of the quantity g^* allows us to replace the assumptions $\log A_1 \geq \frac{\log p}{D}$ and $\log A_2 \geq \frac{\log p}{D}$ occurring in [129] by the weaker (when $p \geq 3$) assumptions $\log A_1 \geq \frac{1}{D}$ and $\log A_2 \geq \frac{1}{D}$.

Set

$$B = \max\Big\{\log\log p + \log B', \frac{10}{D^*}\Big\}$$

and

$$K = \lfloor 2^{12} B g^* (D^*)^3 (\log A_1)(\log A_2) \rfloor, \quad L = \lfloor 16 B D^* \rfloor,$$
$$R_1 = \lceil 4 B g^* (D^*)^2 (\log A_2) \rceil, \quad S_1 = \lceil 4 B g^* (D^*)^2 (\log A_1) \rceil,$$
$$R_2 = \lceil 2^8 B g^* (D^*)^2 (\log A_2) \rceil, \quad S_2 = \lceil 2^8 B g^* (D^*)^2 (\log A_1) \rceil.$$

Since

$$B D^* \geq 10, \quad g^* D^* \geq D, \quad \text{and} \quad g^* (D^*)^2 \geq D^2,$$

we deduce from the assumptions $D \log A_1 \geq 1$ and $D \log A_2 \geq 1$ that K, L, R_1, S_1, R_2, S_2 are greater than 3.

Observe that $R_1 S_1 \geq gL$. Thus, since α_1 and α_2 are multiplicatively independent, there exists a residue class c_1 modulo g such that the first inequality of (12.2) is satisfied.

Observe also that $R_2 S_2 > g(K-1)L$. Consequently, if we furthermore assume that all the elements of the set $\{rb_2 + sb_1 : 0 \leq r < R_2, 0 \leq s < S_2\}$ are distinct, then there exists a residue class c_2 modulo g such that the second inequality of (12.2) is satisfied.

Arguing as in the proof of (11.16), we see that

$$\log b \leq B.$$

Since (12.3) is satisfied, Theorem 12.4 implies the upper bound

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \le 2N + u \le 2^{17} g^* (D^*)^4 (\log A_1)(\log A_2) B^2 + u.$$

By using the upper bounds $g^* \le p^D - 1$ and

$$u \le \frac{\log \min\{b_1, b_2\}}{\log p},$$

we conclude that

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) \le 132000 (p^D - 1)(D^*)^4 (\log A_1)(\log A_2) B^2, \tag{12.9}$$

provided that (12.3) is satisfied.

It remains for us to consider the case where the second inequality of (12.2) is not satisfied. Assume that there is a class c modulo g such that

$$\begin{aligned}\mathrm{Card}\, &\big\{b_1 r + b_2 s : 0 \le r < R_2,\ 0 \le s < S_2,\ m_1 r + m_2 s \equiv c \text{ modulo } g\big\}\\ &< \mathrm{Card}\, \big\{(r, s) : 0 \le r < R_2,\ 0 \le s < S_2,\ m_1 r + m_2 s \equiv c \text{ modulo } g\big\}.\end{aligned}$$

In that situation, we establish a smaller upper bound for $\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2})$ than the right hand side of (12.9).

By Dirichlet's *Schubfachprinzip*, there exists a pair $(r, s) \ne (0, 0)$ of integers such that

$$|r| < R_2, \quad |s| < S_2, \quad b_2 r + b_1 s = 0, \quad m_1 r + m_2 s \equiv 0 \text{ modulo } g.$$

Write

$$\gcd(b_1, b_2) = n = n' p^u,$$

where p does not divide n', and note that

$$b_1 = n r', \quad b_2 = -n s', \quad \text{where } r' = \frac{r}{\gcd(r, s)}, \ s' = \frac{s}{\gcd(r, s)}.$$

Observe that

$$\alpha_1^{b_1} - \alpha_2^{b_2} = \alpha_1^{n r'} - \alpha_2^{-n s'} = \prod_{\xi : \xi^n = 1} (\alpha_1^{r'} - \xi \alpha_2^{-s'}).$$

It follows from Lemma F.5 that

$$\sum_{\substack{\xi : \xi^n = 1 \\ \xi \ne 1}} \mathrm{v}_p(\xi - 1) = u.$$

Arguing as in the proof of Lemma 12.7, there exists a unique n-th root of unity μ in $\overline{\mathbb{Q}}_p$ such that

$$\begin{aligned}&\mathrm{v}_p(\alpha_1^{r'} - \mu \alpha_2^{-s'}) \ge \mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) - u,\\ &\mathrm{v}_p(\alpha_1^{r'} - \mu \alpha_2^{-s'}) > \mathrm{v}_p(\alpha_1^{r'} - \xi \alpha_2^{-s'}), \quad \text{for every } \xi \ne \mu \text{ such that } \xi^n = 1,\end{aligned}$$

as soon as $\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) > \frac{1}{p-1} + u$. Lemma F.6 then shows that μ belongs to the subfield $\mathbb{Q}_p(\alpha_1^{r'}\alpha_2^{s'})$ of $\mathbb{Q}_p(\alpha_1, \alpha_2)$. Thus, we can write $\mu = \zeta^m \xi$, for an integer m and a p^t-th root of unity ξ (recall that ζ is a root of unity of order exactly g). To see this, we use that the class in U/U^1 (here, U denotes the group of units of $\mathbb{Q}_p(\alpha_1, \alpha_2)$ and U^1 its group of principal units) of the component of μ of order prime to p is generated by the classes of α_1 and α_2, and that the order of the p-primary component of μ divides p^t, by the argument based on ramification already used in the proof of Lemma 12.7. Since ξ is in U^1 and the valuation of $\alpha_1^{r'} - \mu\alpha_2^{-s'}$ is positive, the reduction modulo U^1 implies the congruence

$$m_1 r' \equiv -m_2 s' + m \text{ modulo } g.$$

Consequently,

$$m \times \gcd(r, s) \equiv m_1 r + m_2 s \equiv 0 \text{ modulo } g$$

and, setting $g' = g/\gcd(m, g)$, the above congruence shows that $\gcd(r, s)$ is an integer multiple of g'. Thus, we get the upper bounds

$$|r'| \le \frac{R_2 - 1}{g'}, \quad |s'| \le \frac{S_2 - 1}{g'}.$$

Applying Liouville's inequality Theorem B.10 to the polynomial $X - Y$, it follows from (B.3) that

$$\mathrm{v}_p(\alpha_1^{r'} - \mu\alpha_2^{-s'}) \le \frac{[\mathbb{Q}(\alpha_1, \alpha_2, \mu) : \mathbb{Q}]}{e(\log p)} \Big(\log 2 + \frac{R_2 - 1}{g'} h(\alpha_1) + \frac{S_2 - 1}{g'} h(\alpha_2)\Big).$$

Furthermore, since ζ^m is a root of unity of order exactly g', we get

$$\begin{aligned}\frac{[\mathbb{Q}(\alpha_1, \alpha_2, \mu) : \mathbb{Q}]}{e(\log p)} &\le \frac{[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \times [\mathbb{Q}(\zeta^m) : \mathbb{Q}] \times [\mathbb{Q}(\xi) : \mathbb{Q}]}{e(\log p)} \\ &\le \frac{D g' p^{t-1}(p-1)}{e(\log p)} \le \frac{3D^*}{2} g'.\end{aligned}$$

This gives

$$\begin{aligned}\mathrm{v}_p(\alpha_1^{r'} - \mu\alpha_2^{-s'}) &\le \frac{3D^*}{2} (g \log 2 + R_2 \log A_1 + S_2 \log A_2) \\ &\le 2^{10} g B (D^*)^3 (\log A_1)(\log A_2).\end{aligned}$$

Since $g \le p^D - 1$, we obtain a smaller upper bound than in (12.9). We have established Theorem 12.1.

12.5. Deduction of Theorem 12.2 from Theorem 12.5

We have established that, under the assumptions of Theorem 12.5, if the inequality

$$(E + t - 1)(N - K) \ge \frac{D}{2(\log p)} \big(2 \log N + (K - 1) \log b + p^t L\big(Rh(\alpha_1) + Sh(\alpha_2)\big)\big)$$

is satisfied, then

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) < (E + t)N + u.$$

We give an application to the rational case and establish Theorem 12.2. Below, α_1 and α_2 are the rational numbers $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$, respectively. Recall that $t = 0$ if p is odd and that $t = 1$ if $p = 2$. We have shown that, if $E > 2$ and the parameters satisfy

$$(E-1)(N-K) \geq \frac{1}{\log p}\big(2\log N + (K-1)\log b + 4L\big(Rh(\alpha_1) + Sh(\alpha_2)\big)\big),$$

then

$$\mathrm{v}_p(\alpha_1^{b_1} - \alpha_2^{b_2}) < (E + 1)N + u.$$

Using the inequality $E - 1 \geq \frac{2E}{3}$ (which follows from the assumption $E \geq 3$) and

$$\log A_1 \geq \max\{\log|x_1|, \log|y_1|, E\log p\}, \quad \log A_2 \geq \max\{\log|x_2|, \log|y_2|, E\log p\},$$

we choose the various parameters to satisfy the weaker assumption

$$(N-K) \geq \frac{2}{E(\log p)}\big(2\log N + (K-1)\log b + 4L\big(R\log A_1 + S\log A_2\big)\big).$$

Define

$$D^* = \frac{1}{E\log p} \quad \text{and} \quad B = \max\Big\{\log\log p + \log B', \frac{10}{D^*}\Big\}.$$

Check that $\log b \leq B$ and set

$$\begin{aligned} K &= \lfloor 2^{12}Bg(D^*)^3(\log A_1)(\log A_2)\rfloor, \quad L = \lfloor 16BD^*\rfloor,\\ R_1 &= \lceil 4Bg(D^*)^2(\log A_2)\rceil, \quad S_1 = \lceil 4Bg(D^*)^2(\log A_1)\rceil,\\ R_2 &= \lceil 2^8Bg(D^*)^2(\log A_2)\rceil, \quad S_2 = \lceil 2^8Bg(D^*)^2(\log A_1)\rceil. \end{aligned}$$

We proceed as in the proof of Theorem 12.1. We omit the details.

12.6. Deduction of Theorem 12.3 from Theorem 12.1

If a and b are multiplicatively independent, then Theorem 12.3 follows straightforwardly from Theorem 12.1.

If $b = 1$, then choose d in $\{2, 3, 5\}$ such that a and d are multiplicatively independent and p does not divide d. Since the integers ad and d are multiplicatively independent, Theorem 12.3 follows straightforwardly from Theorem 12.1.

If $b > 1$ and a and b are multiplicatively dependent, then there exist positive integers d, r, s such that $a = d^r$ and $b = d^s$. We then have

$$\mathrm{v}_p(a^{p-1} - b^{p-1}) = \mathrm{v}_p(d^{(r-s)(p-1)} - 1),$$

and we are now in the case $b = 1$. Since $d^{r-s} \leq a$, the result follows.

Chapter 13
Open problems

We collect in this chapter a list of open questions and conjectures in the theory of linear forms in logarithms or somehow related to their applications. Some of them have been extracted from Waldschmidt's survey [434] of open Diophantine problems, to which the reader is also directed. We take the opportunity to highlight several questions which are slightly aside the main topic of this book.

13.1. Classical conjectures in transcendence theory

We start with a conjectural analogue of Theorem 1.2 for the logarithm function, generalising Theorem 1.4. Recall that the complex numbers $z_1, \dots, z_n$ are algebraically independent if no non-zero polynomials in n variables with algebraic coefficients vanish at the point $(z_1, \dots, z_n)$.

Conjecture 13.1. *Let $n \geq 2$ be an integer. Let $\alpha_1, \dots, \alpha_n$ be non-zero algebraic numbers and $\log \alpha_1, \dots, \log \alpha_n$ any determinations of their logarithms. If $\log \alpha_1, \dots, \log \alpha_n$ are linearly independent over the rationals, then $\log \alpha_1, \dots, \log \alpha_n$ are algebraically independent over the rationals.*

It is not yet known whether log 2 and log 3 are algebraically independent.

We display two celebrated extensions of Conjecture 13.1. A first one, the Schanuel conjecture, contains any reasonable transcendence conjecture dealing with values of the exponential function.

Conjecture 13.2 (Schanuel). *Let $z_1, \dots, z_n$ be complex numbers, linearly independent over the rationals. Then at least n of the $2n$ numbers $z_1, \dots, z_n, \mathrm{e}^{z_1}, \dots, \mathrm{e}^{z_n}$ are algebraically independent over the rationals.*

Conjecture 13.1 is a special case of Schanuel's conjecture (assume that the n numbers $\mathrm{e}^{z_1}, \dots, \mathrm{e}^{z_n}$ are algebraic). Another special case is the Lindemann–Weierstrass Theorem 1.2, which corresponds to the case where $z_1, \dots, z_n$ are algebraic.

Another kind of open problems deals with measures of linear independence. We point out a conjecture of Lang, quoted as Conjecture 1.11 in [432].

Conjecture 13.3. *For any positive ε, there exists a positive real number $c(\varepsilon)$ such that, for any non-zero rational integers $a_1, \dots, a_n, b_1, \dots, b_n$ with $a_1^{b_1} \cdots a_n^{b_n} \neq 1$, we have*

$$|a_1^{b_1} \cdots a_n^{b_n} - 1| \geq \frac{c(\varepsilon)^n}{B^{n-1+\varepsilon} A^{n+\varepsilon}},$$

where $A = \max\{|a_1|, \dots, |a_n|, 2\}$ and $B = \max\{|b_1|, \dots, |b_n|, 2\}$.

Conjecture 13.3 is likely to be out of reach. Recall that, under its assumption, the current best known estimate (Theorem 2.2) takes the form

$$\log |a_1^{b_1} \cdots a_n^{b_n} - 1| \geq -C^n (\log |2a_1|) \dots (\log |2a_n|) (\log B), \tag{13.1}$$

for an effectively computable positive real number C (note that $c(\varepsilon)$ is not required to be effectively computable in Conjecture 13.3). It would be of greatest interest to replace the product $(\log |2a_1|) \dots (\log |2a_n|)$ in (13.1) by some smaller quantity (say, by $\log A$), even if we get a weaker dependence on B (as long as it remains $o(B)$).

We conclude this short section with a particular case of the four exponential conjecture.

Problem 13.4. *Does there exist an irrational number t such that 2^t and 3^t are both rational integers?*

We know that there are no irrational number t for which 2^t, 3^t, and 5^t are all rational integers. This statement is a particular case of the *six exponentials theorem*, which occurred for the first time in a paper by Alaoglu and Erdős [4] and can also be deduced from a more general result of Schneider [361]; see Section 1.4 of [432] for additional references.

13.2. Diophantine equations

By applying estimates for linear forms in logarithms, Stark [390] proved that, for every positive ε, we have

$$|x^3 - y^2| \gg_\varepsilon (\log x)^{1-\varepsilon}.$$

The current best lower bound for the difference between squares and cubes, namely

$$|x^3 - y^2| \gg \frac{\log x}{(\log \log x)^4},$$

was obtained by Juricevic [234]. This lower bound is considerably far away from what is predicted by a conjecture of Hall [219] (see Lang [250, p. 213] for a generalization).

Problem 13.5 (Hall's conjecture). *There exists a positive real number C such that for all positive integers x and y with $x^3 \neq y^2$ we have*

$$|x^3 - y^2| > C\,\sqrt{x}.$$

Danilov [160] proved that $0 < |x^3 - y^2| < 0.97\sqrt{x}$ has infinitely many solutions in positive integers x, y; see also [173] and the references given therein. According to Elkies [176], Hall's conjecture is likely not to hold, and should be replaced by the weaker formulation

"*For any positive ε, there exists a positive number $C(\varepsilon)$ such that for all positive integers x and y with $x^3 \neq y^2$ we have $|x^3 - y^2| > C(\varepsilon)\,\sqrt{x^{1-\varepsilon}}$.*"

For the difference between higher powers, see [66, 161, 435].

We reproduce Problem 1.1 of [434].

Problem 13.6. *Let $f(X,Y)$ be an integer polynomial such that the equation $f(x,y)=0$ has only finitely many solutions in integers x,y. Give an effectively computable upper bound, depending only on the degree of $f(X,Y)$ and of the maximal absolute value of its coefficients, for the absolute values of the integers x and y satisfying $f(x,y)=0$.*

We have seen in Chapter 4 partial solutions of Problem 13.6, for instance when $f(X,Y)$ is of the form $g(X,Y)+a$, where a is a non-zero integer and $g(X,Y)$ is homogeneous and such that $g(X,1)$ has at least three distinct roots.

The following open problem has been posed by Schinzel and Tijdeman [375].

Problem 13.7. *Let $P(X)$ be a polynomial with rational coefficients and at least three simple roots. Then, the equation $P(x)=y^2z^3$ has only finitely many solutions in non-zero integers x,y,z.*

We formulate under a slightly different form a conjecture of Shorey [371].

Problem 13.8 (Shorey's conjecture). *Let $L\geq 2$ be an integer and $m_1,\ldots,m_{L-1}$ integers with $m_1>m_2>\cdots>m_{L-1}>0$. Let $f(X)=b_1X^{m_1}+\cdots+b_{L-1}X^{m_{L-1}}+b_L$ be a polynomial of degree m_1 with rational coefficients. Assume that $f(X)$ has distinct roots and that b_L is non-zero. Denote by H an upper bound for the absolute values of the numerators and denominators of $b_1,\ldots,b_L$. Let x, y, and n be integers with $n\geq 2$, $|y|\geq 2$ and*

$$f(x)=y^n.$$

Then, there exists an integer n_0, depending only on H and L, such that either

$$n\leq n_0$$

or

$$y^n-f(x)=y^n-b_1x^{m_1}-\cdots-b_{L-1}x^{m_{L-1}}-b_L$$

has a proper subsum which vanishes.

Shorey observed that the assumptions on $f(X)$ in the above conjecture are necessary, and that the integer n_0 has to depend on H and on L. It is not difficult to see that Shorey's conjecture is a generalization of the Pillai conjecture, mentioned in Section 4.8 and reproduced below.

Problem 13.9 (Pillai's conjecture). *Let a, b, and k be non-zero integers. Then, the Diophantine equation*

$$ax^m-by^n=k,\quad \textit{in integers } m, n, x, y, \textit{ with } m\geq 3,\ n\geq 2,\ x\geq 2, \textit{ and } y\geq 2,$$

has only finitely many solutions.

Nair [314] established that the Pillai conjecture is true if there exist positive real numbers C and δ such that $|x^3-y^2|>C\,x^\delta$ holds for any positive integers x and y with $x^3\neq y^2$.

Equal binomial coefficients have been considered by de Weger [437]; see also [80] and the references given therein.

Problem 13.10. *Find all the integers n, k, m, ℓ with*

$$2 \le k \le \frac{n}{2}, \quad 2 \le \ell \le \frac{m}{2}, \quad k < l, \quad \textit{and} \quad \binom{n}{k} = \binom{m}{\ell}.$$

Theorem 3.14 asserts that 0, 1, 8, and 144 are the only perfect powers in the Fibonacci sequence. The following question is much more complicated.

Problem 13.11. *Determine all the perfect powers in the Tribonacci sequence $(T_n)_{n\in\mathbb{Z}}$ defined by $T_0 = T_1 = 0$, $T_2 = 1$, and $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ for n in $\mathbb{Z}$.*

We know that 27 is the only perfect power equal to a square plus 2 (see Section 4.6), but we do not know whether there exist perfect powers equal to a square minus 2.

Problem 13.12. *Determine all the integer solutions (x, y, n) of the equation $x^2 - 2 = y^n$.*

Problem 13.12 is difficult since $x^2 - 2 = y^n$ has the solution $1^2 - 2 = (-1)^n$ for every odd integer n. Siksek [378] showed how estimates for linear forms in two logarithms can be combined with other arguments to show that if $x^2 - 2 = y^n$ holds with n prime and $y \ge 2$, then n is less than 1237.

There are only very few results on the distribution of perfect powers. As already pointed out in Section 4.8, the following question remains unsolved.

Problem 13.13. *Does the difference between two consecutive perfect powers tend to infinity?*

The next problem remains open, even though conjecturally 25 is the only perfect power n such that $n + 2$ is also a perfect power.

Problem 13.14. *Prove that there exists a positive constant k for which there are only finitely many integers n such that n, $n + 2, \ldots, n + 2k$ are perfect powers.*

It is very likely that

$$\frac{3^5 - 1}{3 - 1} = 11^2, \quad \frac{7^4 - 1}{7 - 1} = 20^2, \quad \text{and} \quad \frac{18^3 - 1}{18 - 1} = 7^3$$

are the only solutions to the Nagell–Ljunggren equation; see the survey [133].

Problem 13.15. *The Nagell–Ljunggren equation*

$$\frac{x^n - 1}{x - 1} = y^q, \quad \textit{in integers } n \ge 3,\ q \ge 2,\ x \ge 2,\ y \ge 2,$$

has only finitely many solutions.

The next open question asks for an extension of some results established in Section 6.5.

Problem 13.16. *If a, b, c, d, y, and q are integers with $a > b > c > d > 0$, $y \ge 2$, and*

$$2^a + 2^b + 2^c + 2^d + 1 = y^q,$$

then prove that q is bounded. Solve the Diophantine equation

$$2^a + 2^b + 7 = y^q,$$

in integers a, b, y, q with $a > b > 0$, $y \ge 2$, and $q \ge 2$.

We conclude this section with two open questions on upper bounds for the number of solutions to certain Diophantine equations.

PROBLEM 13.17. *Let D, k, and p be positive integers with p prime and* $\gcd(D, kp) = 1$. *Does there exist an upper bound for the number of solutions of the Diophantine equation*

$$x^2 + D = k\,p^n, \quad \textit{in integers } x \geq 1, n \geq 1,$$

which does not depend on D, k, and p?

The next problem reproduces a conjecture of Schmidt [358].

PROBLEM 13.18. *Let $F(X, Y)$ be an integer polynomial of naïve height H and total degree d, such that the equation $F(x, y) = 0$ defines an irreducible curve of positive genus. Let $N(F)$ denote the number of pairs (x, y) of integers with $F(x, y) = 0$. Prove that, for every positive real number ε, there exists a real number $c(d, \varepsilon)$, depending only on d and ε, such that $N(F) < c(d, \varepsilon)\, H^{\varepsilon}$.*

Problem 13.18 remains open even for very special families of polynomials, including the polynomials $Y^2 - X^3 - A$ with varying integer A; see [67, 170, 225, 339].

13.3. Miscellaneous

The next problem addresses the number of perfect powers in short intervals.

PROBLEM 13.19. *For any positive real number x and any positive integer n, let $\Xi(n, x)$ denote the number of perfect powers in $[n, n + x]$ and set*

$$\Xi(x) = \limsup_{n \to +\infty} \Xi(n, x).$$

Give an upper bound for $\Xi(x)$.

Using sieve methods, it is possible to prove that $\Xi(x) \ll x/(\log x)$. Presumably, this upper estimate is very far from the true order of magnitude of Ξ. It is even likely that $\Xi(x) = 1$ for any $x \geq 1$. Such a result would follow from Pillai's conjecture. Slightly related problems have been considered by de Weger and van de Woestijne [438, 439].

Mahler [281] proved that $\|e^n\| > n^{-40n}$ and $\|\log n\| \geq n^{-40 \log\log n}$ hold for every sufficiently large integer n; see [224] for the best known lower bounds to date, [248, 431], and Section 4 of [433].

PROBLEM 13.20. *Prove that there exists a real number C such that*

$$\|e^n\| > e^{-Cn} \quad \textit{and} \quad \|\log n\| > n^{-C}$$

hold for every integer $n \geq 2$.

To solve Problem 13.20 we need to improve the current lower bounds for the inhomogeneous linear form $|b_0 - \log b_1|$, where b_0 and b_1 are integers greater than 2.

We reproduce Grimm's conjecture [204].

PROBLEM 13.21 (Grimm's conjecture). *Let n, k be positive integers such that $n + 1, \dots, n+k$ are composite. Then, there exist k distinct prime numbers $p_1, \dots, p_k$ such that $n + j$ is divisible by p_j for $j = 1, \dots, k$.*

The theory of linear forms in logarithms has been applied to Grimm's conjecture by Ramachandra, Shorey, and Tijdeman [341, 342].

In the statement of Theorem 6.3, the effectively computable real number $\tau(\xi, b)$ depends on ξ and b. It is likely that a stronger statement holds.

Problem 13.22. *For every integer $b \geq 2$ and every quadratic real number ξ, there exists a positive, effectively computable real number τ, depending only on ξ (and not on b), such that*

$$\|b^n \xi\| \gg_{\xi,b} b^{-(1-\tau)n}, \quad \textit{for } n \geq 1.$$

Approximation to algebraic numbers by rational numbers whose denominator is a perfect power was considered by Pethő [322].

Problem 13.23. *Let α be an irrational algebraic number. Let $k \geq 2$ be an integer. Prove that there exist effectively computable positive real numbers q_0, ε such that*

$$\|q^k \alpha\| > q^{-k+\varepsilon}, \quad \textit{for } q > q_0.$$

As mentioned in Sections 6.2 and 6.12, Inequality (6.5) and, consequently, the equality $g(n) = 2^n + \lfloor (3/2)^n \rfloor - 2$ hold for every sufficiently large integer n.

Problem 13.24. *Give an upper bound for the number of positive integers n such that*

$$\left\| \left(\frac{3}{2}\right)^n \right\| < \left(\frac{3}{4}\right)^{n-1}.$$

Upper bounds for the number of solutions to (A.2), given for instance in [181], do not seem to be sufficient to solve Problem 13.24.

Theorem 6.2 gives an effective lower bound for the fractional part of powers of rational numbers. It would be of interest to extend it to powers of algebraic numbers.

Problem 13.25. *Let α be a real algebraic irrational number larger than 1 and n a positive integer. Give an effective lower bound for $\|\alpha^n\|$.*

The next problem is Question 6.2 of [249], which proposes an extension of Theorem 6.2.

Problem 13.26. *Let $k \geq 2$ and $q, a_1, \ldots, a_k$ be integers with $\gcd(q, a_1, \ldots, a_k) = 1$ and $2 \leq q < a_i$ for $i = 1, \ldots, k$. Is there an effectively computable positive real number τ such that*

$$\left\| \frac{a_1^n + \cdots + a_k^n}{q^n} \right\| > \frac{1}{2q^{(1-\tau)n}}, \quad \textit{for } n \geq 1?$$

We point out an open problem from [115]; see also [370].

Problem 13.27. *Let ξ be a real algebraic number of degree at least three. Let $(p_n/q_n)_{n \geq 1}$ denote the sequence of its convergents. Find an effective lower bound for $P[p_n]$ and for $P[q_n]$.*

An important open problem addresses effective estimates for the growth of integer linear recurrence sequences. Obviously, if $(u_n)_{n \geq 0}$ is a non-degenerate recurrence sequence of integers with a dominant root α, then $|u_n|$ grows as $n^\ell |\alpha^n|$ for some integer ℓ. When there is no dominant root and α is a root of maximal modulus, Evertse [180] and, independently, van der Poorten and Schlickewei [337] established that, for any positive ε, there exists an integer n_0 such that $|u_n| > |\alpha|^{(1-\varepsilon)n}$ for every $n > n_0$. The proof is based on the Schmidt subspace theorem and, consequently, does not yield an effective estimate for n_0.

Problem 13.28. *Let $(u_n)_{n\geq 0}$ be a non-degenerate recurrence sequence of integers. Find an effective lower bound for $|u_n|$.*

When there are no more than three roots of maximal modulus, Problem 13.28 has been solved by Mignotte [293] (when these roots are simple) and by Mignotte, Shorey, and Tijdeman [299] (in the general case).

The preceding problem is closely connected to the well-known Skolem problem.

Problem 13.29 (Skolem's problem). *Is the question* "does a given non-degenerate recurrence sequence of integers have a zero?" *decidable?*

The answer to Problem 13.29 is positive for recurrence sequences of order at most 4, see [299, 424], but not yet known for recurrence sequences of order 5. For example, it is pointed out in [164] that we still cannot find an effectively computable integer n_0 such that u_n is non-zero for every integer n greater than n_0, where

$$u_n = (8+\mathrm{i})^n + (8-\mathrm{i})^n - (7+4\mathrm{i})^n - (7-4\mathrm{i})^n - 1.$$

Other decision problems for linear recurrence sequences have been investigated, including the *Positivity problem* ("Given a non-degenerate recurrence sequence of integers, are all of its terms positive?") and the *Ultimate positivity problem* ("Given a non-degenerate recurrence sequence of integers, are all but finitely many of its terms positive?"); see [319, 320] and the references therein.

We reproduce Lehmer's problem, discussed in Section 10.1.

Problem 13.30 (Lehmer's problem). *There exists a positive real number c such that every non-zero algebraic number α of degree d which is not a root of unity satisfies*

$$h(\alpha) \geq \frac{c}{d}.$$

Amoroso and David [8] have extended Lehmer's problem to simultaneous approximation and established a slightly weaker version of it.

Problem 13.31. *Let n be a positive integer. There exists a positive real number $c(n)$ such that if $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent algebraic numbers and D denotes the degree of the extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}$, then*

$$\prod_{i=1}^{n} h(\alpha_i) \geq \frac{c(n)}{D}.$$

See [10] for the currently best known result towards Problem 13.31 and [9, 344] for related results and problems.

Appendices

Appendix A
Approximation by rational numbers

This appendix is devoted to classical results on the approximation to real numbers by rational numbers. We mostly omit the proofs and refer the reader to a text of van der Poorten [336] and to the books of Bugeaud [113], Cassels [144], Hardy and Wright [220], Khintchine [239], Perron [321], and Schmidt [357], among many others.

Let $a_0, a_1, \ldots$ be integers with $a_1, a_2, \ldots$ positive. A *finite continued fraction* denotes any expression of the form

$$[a_0; a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}.$$

We call any expression of the above form or of the form

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots}}} = \lim_{n \to +\infty} [a_0; a_1, a_2, \ldots, a_n]$$

a *continued fraction*. The above limit always exists.

Any rational number r has exactly two different continued fraction expansions. These are $[r]$ and $[r-1;1]$ if r is an integer and, otherwise, one of them reads $[a_0; a_1, \ldots, a_{n-1}, a_n]$ with $a_n \geq 2$, and the other one is $[a_0; a_1, \ldots, a_{n-1}, a_n - 1, 1]$. Any irrational number has a unique expansion in continued fraction.

Theorem A.1. *Let $\xi = [a_0; a_1, a_2, \ldots]$ be an irrational number. Let n be a positive integer. Set $\frac{p_n}{q_n} := [a_0; a_1, a_2, \ldots, a_n]$ with p_n and q_n non-negative and coprime. Putting*

$$p_{-1} = 1, \quad q_{-1} = 0, \quad p_0 = a_0, \quad \text{and} \quad q_0 = 1,$$

we have

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2},$$

and

$$p_{n-1} q_n - p_n q_{n-1} = (-1)^n.$$

Furthermore, we have

$$\frac{1}{(a_{n+1}+2)q_n^2} < \frac{1}{q_n(q_n+q_{n+1})} < \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{a_{n+1}q_n^2} \le \frac{1}{q_n^2}. \qquad \text{(A.1)}$$

With the notation of Theorem A.1, the rational number $\frac{p_n}{q_n}$ is called the n-th convergent to ξ. The next theorem, established by Legendre [257], gives a sufficient condition for a rational number to be a convergent of a given real number.

Theorem A.2. *Let ξ be a real number. Any non-zero rational number $\frac{a}{b}$ with*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}.$$

is a convergent of ξ.

The irrationality exponent of an irrational number ξ measures the quality of approximation to ξ by rational numbers.

Definition A.3. Let ξ be an irrational real number. The real number μ is an irrationality measure for ξ if there exists a positive real number $C(\xi)$ such that every rational number $\frac{p}{q}$ with $q \ge 1$ satisfies

$$\left|\xi - \frac{p}{q}\right| > \frac{C(\xi)}{q^{\mu}}.$$

If, moreover, the constant $C(\xi)$ is effectively computable, then μ is an effective irrationality measure for ξ. We denote by $\mu(\xi)$ (*resp.,* $\mu_{\mathrm{eff}}(\xi)$) the infimum of the irrationality measures (*resp.,* effective irrationality measures) for ξ and call it the irrationality exponent (*resp.,* effective irrationality exponent) of ξ.

Clearly, $\mu_{\mathrm{eff}}(\xi)$ is always larger than or equal to $\mu(\xi)$. It follows from (A.1) and Theorem A.2 that the irrationality exponent of ξ can be read off its continued fraction expansion. Many authors attribute to Dirichlet [166] the first statement of Theorem A.4, which was, however, known long before 1842, since it directly follows from the theory of continued fractions. Throughout this chapter, “almost every” always refers to the Lebesgue measure.

Theorem A.4. *Every irrational real number ξ satisfies $\mu(\xi) \ge 2$, with equality for almost every ξ.*

Proof. The first assertion follows from (A.1). Let ε be a positive real number. The set

$$\bigcap_{Q\ge 1} \bigcup_{q \ge Q} \bigcup_{p=0}^{q} \Big(\frac{p}{q} - \frac{1}{q^{2+\varepsilon}}, \frac{p}{q} + \frac{1}{q^{2+\varepsilon}}\Big)$$

has zero Lebesgue measure, since the sum $\sum_{q\ge Q} q^{-1-\varepsilon}$ tends to 0 as Q tends to infinity. This shows that the set of real numbers in $(0,1)$ whose irrationality exponent exceeds $2+\varepsilon$ has zero Lebesgue measure. This implies the second assertion of the theorem. □

The next result was proved in 1844 by Liouville [264].

Theorem A.5 (Liouville's theorem). *Let ξ be an irrational algebraic number of degree d. The inequality*

$$\left|\xi - \frac{p}{q}\right| \gg_\xi \frac{1}{q^d}$$

holds for all rational numbers $\frac{p}{q}$ with $q \geq 1$. Consequently, we have

$$\mu_{\text{eff}}(\xi) \leq d.$$

Proof. Let $\frac{p}{q}$ be a rational number with $|\xi - \frac{p}{q}| < 1$. Let $P(X)$ be the minimal defining polynomial of ξ over the rational integers. Since it is irreducible, we have $P(\frac{p}{q}) \neq 0$ and $|q^d P(\frac{p}{q})| \geq 1$. By Rolle's theorem, there exists a real number t_0, lying between ξ and $\frac{p}{q}$, such that

$$\left|P\left(\frac{p}{q}\right)\right| = \left|P(\xi) - P\left(\frac{p}{q}\right)\right| = \left|\xi - \frac{p}{q}\right| \times |P'(t_0)|.$$

Consequently, we have $|t_0 - \xi| \leq 1$ and

$$\left|\xi - \frac{p}{q}\right| \geq \frac{1}{q^d \ \max\{|P'(t)| : \xi - 1 \leq t \leq \xi + 1\}}.$$

This concludes the proof. □

Definition A.6. A real number ξ is called a Liouville number if $\mu(\xi)$ is infinite.

It follows from Theorem A.5 that every Liouville number is transcendental. By combining Theorems A.4 and A.5, we immediately get that the effective irrationality exponent of every quadratic real number is equal to 2.

Roth's celebrated theorem [349], established in 1955, asserts that, from the point of view of rational approximation, an irrational real algebraic number behaves like almost every real number.

Theorem A.7 (Roth's theorem). *Every irrational real algebraic number ξ satisfies $\mu(\xi) = 2$.*

We point out that we do not know any example of a real algebraic number of degree at least three and whose effective irrationality exponent is equal to 2. However, for any given positive ε, there are explicit examples of real algebraic numbers ξ with $\mu_{\text{eff}}(\xi) \leq 2 + \varepsilon$; see e.g. [89, 90].

The next theorem, established in 1957 by Ridout [346], is aside the main topic of this book; however, it is referred to at several places. Recall that for a prime number ℓ and a non-zero integer a, we write $|a|_\ell$ for the inverse of the greatest power of ℓ which divides a.

Theorem A.8 (Ridout's theorem). *Let ξ be a real algebraic number, S a finite set of prime numbers, and ε a positive real number. Then, there are only finitely many rational numbers $\frac{p}{q}$ with $q \geq 1$ and*

$$\prod_{\ell \in S} |pq|_\ell \left|\xi - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}. \tag{A.2}$$

Theorem A.7 corresponds to Theorem A.8 applied with an empty set S. Observe that the product $\prod_{\ell \in S} |pq|_\ell$ in (A.2) is always at most equal to 1.

The Roth theorem has been extended by Schmidt to systems of n linear forms in n variables with algebraic coefficients (Theorem A.7 deals with the case $n = 2$): this is the Schmidt subspace theorem. A complete proof of it can be found in [357]; see also Chapter 7 of [88].

Appendix B
Heights

This appendix starts with basic results on absolute values and the elementary theory of heights. We omit most of the proofs and direct the reader to Chapter 1 of [88], Chapter 1 of [183], or Chapter 3 of [432] for a more detailed exposition; see also [315] for the theory of valuations. We largely follow the presentation of [432] to define the Weil height of a complex algebraic number. The second section is devoted to a general form of the Liouville inequality and this appendix ends with an elementary estimate for a linear form in one p-adic logarithm.

B.1. Definitions

Let α be a complex algebraic number of degree $d \geq 1$ with minimal defining polynomial

$$f(X) := a_d X^d + \cdots + a_1 X + a_0 = a_d (X - \alpha_1) \cdots (X - \alpha_d) \qquad \text{(B.1)}$$

over $\mathbb{Z}$, where $\alpha = \alpha_1$ and $\alpha_1, \ldots, \alpha_d$ are the Galois conjugates of α. Set $k = \mathbb{Q}(\alpha)$ and let M_k denote the set of places of k. To each complex embedding $\sigma\colon k \longrightarrow \mathbb{C}$ we associate a complex absolute value v_σ defined by $|x|_{v_\sigma} = |\sigma(x)|$ for x in k. Conversely, let v be a complex absolute value on k, which coincides with the ordinary absolute value on the set of positive rational numbers. The completion k_v of k is an extension of the completion $\mathbb{R}$ of $\mathbb{Q}$, hence it is equal to $\mathbb{R}$ or $\mathbb{C}$. We denote by d_v the degree $[k_v : \mathbb{R}]$ and observe that

$$d_v = \begin{cases} 1, & \text{if } v \text{ is real,} \\ 2, & \text{if } v \text{ is complex.} \end{cases}$$

To a real absolute value v corresponds one and only one real embedding of k, while two (complex conjugate) embeddings of k into $\mathbb{C}$ correspond to a complex non-real absolute value v. We deduce that the number of elements in the set M_k^∞ of infinite places of k (i.e. the number of non-equivalent Archimedean absolute values of k) is $r = r_1 + r_2$, where r_1 is the number of real roots of $f(X)$ and r_2 is the number of pairs of conjugate complex roots of $f(X)$. Observe that $d = r_1 + 2r_2$ and

$$d = \sum_{v \in M_k^\infty} d_v.$$

The d-tuple $\bigl(|\alpha_1|, \dots, |\alpha_d|\bigr)$ consists of the elements $|\alpha|_v$, $v \in M_k^\infty$, where each $|\alpha|_v$ is repeated d_v times. It follows from (B.1) that

$$\prod_{v \in M_k^\infty} |\alpha|_v^{d_v} = \prod_{i=1}^{d} |\alpha_i| = \left|\frac{a_0}{a_d}\right| \tag{B.2}$$

and

$$\prod_{v \in M_k^\infty} \max\{1, |\alpha|_v\}^{d_v} = \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Let p be a prime number. Since the p-adic field $\mathbb{Q}_p$ is complete, the absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ normalized such that $|p|_p = p^{-1}$ has a unique extension to any finite extension K of $\mathbb{Q}_p$. This extension is given as follows. For γ in K, let $\mathrm{Norm}_{K/\mathbb{Q}_p}(\gamma)$ denote the norm of the $\mathbb{Q}_p$-endomorphism of K which maps x onto γx. If d is the degree of K over $\mathbb{Q}_p$, then the extension $|\cdot|_p$ of the p-adic absolute value of $\mathbb{Q}_p$ to K is defined by

$$|\gamma|_p = |\mathrm{Norm}_{K/\mathbb{Q}_p}(\gamma)|_p^{1/d}.$$

Furthermore, if γ is non-zero, its p-adic valuation is given by

$$\mathrm{v}_p(\gamma) = -\frac{\log|\gamma|_p}{\log p} = -\frac{1}{d}\,\frac{\log|\mathrm{Norm}_{K/\mathbb{Q}_p}(\gamma)|_p}{\log p},$$

which is a non-negative rational number whose denominator divides d. The *ramification index* e_K of K over $\mathbb{Q}_p$ is the index of $\mathbb{Z}$ in the subgroup $\mathrm{v}_p(K \setminus \{0\})$ of $\frac{1}{d}\mathbb{Z}$. The *residue degree* of K over $\mathbb{Q}_p$ is the quotient $f_K := d/e_K$.

Denote by $\overline{\mathbb{Q}}_p$ the algebraic closure of $\mathbb{Q}_p$, equipped with the absolute value $|\cdot|_p$. The field $\overline{\mathbb{Q}}_p$ is not complete (this makes a difference with the Archimedean situation). We denote by $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}}_p$ for $|\cdot|_p$. This is a complete field in which $\overline{\mathbb{Q}}_p$ is dense, and moreover $\mathbb{C}_p$ is algebraically closed.

Let α be a complex algebraic number of degree $d \geq 1$ with minimal defining polynomial

$$f(X) := a_d X^d + \cdots + a_1 X + a_0 = a_d(X - \alpha_1^{(p)}) \cdots (X - \alpha_d^{(p)})$$

over $\mathbb{Z}$, where $\alpha_1^{(p)}, \dots, \alpha_d^{(p)}$ denote the roots of $f(X)$ in $\mathbb{C}_p$. Set $k = \mathbb{Q}(\alpha)$. There are d distinct embeddings of k into $\mathbb{C}_p$ (each of them maps a root of $f(X)$ onto another root of $f(X)$). With each such embedding $\sigma\colon k \longrightarrow \mathbb{C}_p$ we associate an ultrametric absolute value v_σ dividing p defined by $|x|_{v_\sigma} = |\sigma(x)|_p$.

Let v be an absolute value on k which extends the p-adic absolute value of $\mathbb{Q}$. We view the completion k_v of k as an extension of $\mathbb{Q}_p$ and denote by α_v the image of α in k_v. Then $\mathbb{Q}_p(\alpha_v)$ is a finite extension of $\mathbb{Q}_p$. We can say more about the degree of this extension. Write the factorisation of $f(X)$ into irreducible polynomials in $\mathbb{Q}_p[X]$ as $f(X) = \overline{f}_1(X) \cdots \overline{f}_r(X)$. Notice that the number r of irreducible factors depends on the prime number p and that, since $f(X)$ is irreducible in $\mathbb{Q}[X]$, the polynomials $\overline{f}_1(X), \dots, \overline{f}_r(X)$ in $\mathbb{Q}_p[X]$ are pairwise distinct. Since α_v is a root of $f(X)$ in $\mathbb{C}_p$, there is a unique i, with $1 \leq i \leq r$, such that α_v is a root of $\overline{f}_i(X)$. Therefore $\overline{f}_i(X)$

has a root in the field $\mathbb{Q}_p(\alpha_v)$, which is an extension of $\mathbb{Q}_p$ of degree $d_v = \deg(\overline{f_i})$, and $k_v = \mathbb{Q}_p(\alpha_v)$. The integer d_v is called *the local degree* at v. From this it follows that k_v is isomorphic to a subfield of $\mathbb{C}_p$, and we get an embedding σ_v of k into $\mathbb{C}_p$ such that $v_{\sigma_v} = v$. Hence the mapping $\sigma \mapsto v_\sigma$ is surjective.

The number of distinct embeddings of k into $\mathbb{C}_p$ associated to a given absolute value v dividing p is the local degree $d_v = [k_v : \mathbb{Q}_p]$ of v, and the number of places v in M_k with v dividing p is the number of irreducible factors of $f(X)$ over $\mathbb{Q}_p$. Let e_v and f_v denote respectively the ramification index and the residue degree of k_v over $\mathbb{Q}_p$. Then, we have

$$d_v = e_v f_v$$

and

$$d = \sum_{v \in M_k, v|p} d_v = \sum_{v \in M_k, v|p} e_v f_v.$$

Let O_k be the ring of integers of k. The integer ideal pO_k factors in k as a product of prime ideals and can be written as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where e_j is the *ramification index* of the prime ideal $\mathfrak{p}_j$ for $j = 1, \dots, r$ and the integer r is the number of irreducible polynomials in the factorisation of $f(X)$ in $\mathbb{Q}_p[X]$. Let $j = 1, \dots, r$ and α be a non-zero algebraic number in k. Let $\mathrm{v}_{\mathfrak{p}_j}(\alpha)$ denote the exponent of $\mathfrak{p}_j$ in the factorisation of the fractional ideal αO_k in a product of prime ideals. Let v_j be the absolute value of k associated with the prime ideal $\mathfrak{p}_j$. The completion $k_{\mathfrak{p}_j} = k_{v_j}$ of k with respect to the absolute value v_j is a finite extension of the p-adic field $\mathbb{Q}_p$. Its ramification index is the ramification index of the ideal $\mathfrak{p}_j$ and its degree is the degree of the polynomial $\overline{f_{v_j}}(X)$. Furthermore, f_{v_j} is the degree of the field $O_k/\mathfrak{p}_j$ over $\mathbb{Z}/p\mathbb{Z}$ and it is called the *residue degree* of $k_{\mathfrak{p}_j}$. The norm over $\mathbb{Q}$ of the ideal $\mathfrak{p}_j$, denoted by $\mathrm{Norm}_{k/\mathbb{Q}}\, \mathfrak{p}_j$, is equal to $p^{f_{v_j}}$. The field $k_{\mathfrak{p}_j}$ is isomorphic to the extension of the field $\mathbb{Q}_p$ by a root of the irreducible polynomial $\overline{f_{v_j}}(X)$ and we have

$$|\alpha|_{v_j}^{d_{v_j}} = (\mathrm{Norm}_{k/\mathbb{Q}}\, \mathfrak{p}_j)^{-\mathrm{v}_{\mathfrak{p}_j}(\alpha)}. \tag{B.3}$$

If Ψ denotes this isomorphism, then the valuation $\mathrm{v}_p^{(j)}$ defined by

$$\mathrm{v}_p^{(j)}(\alpha) = \frac{\mathrm{v}_{\mathfrak{p}_j}(\alpha)}{e_j},$$

which extends to the algebraic number field k the valuation v_p defined on $\mathbb{Q}$, satisfies $\mathrm{v}_p^{(j)}(\alpha) = \mathrm{v}_p(\Psi(\alpha))$. With a slight abuse of notation, we denote the latter quantity by $\mathrm{v}_p(\alpha)$.

Warning B.1. Through this book, we use v_p, without any superscript, to denote a p-adic valuation on a complex algebraic number field. We also use the same notation v_p to denote the unique extension to $\mathbb{C}_p$ of the p-adic valuation. This should not cause any confusion.

Any ideal $\mathfrak{a}$ of k factors uniquely as a product of powers of prime ideals of O_k and its norm $\mathrm{Norm}_{k/\mathbb{Q}}\, \mathfrak{a}$ is then defined by multiplicativity. Furthermore, if α is a non-zero algebraic number in k, then the norm (over $\mathbb{Q}$) of the ideal αO_k is the absolute value of the norm (over $\mathbb{Q}$) of α, defined as the product of its Galois conjugates.

The d-tuple $\big(|\alpha_1^{(p)}|_p, \ldots, |\alpha_d^{(p)}|_p\big)$ consists of the elements $|\alpha|_v$, where v in M_k divides p and each $|\alpha|_v$ is repeated d_v times. In particular, we get

$$\prod_{v \in M_k, v | p} |\alpha|_v^{d_v} = \prod_{i=1}^{d} |\alpha_i^{(p)}|_p = \left| \frac{a_0}{a_d} \right|_p \tag{B.4}$$

and

$$\prod_{v \in M_k, v | p} \max\{1, |\alpha|_v\}^{d_v} = \prod_{i=1}^{d} \max\{1, |\alpha_i^{(p)}|_p\}.$$

The proof that the latter quantity is equal to $\frac{1}{|a_d|_p}$ is left as an exercise for the reader; see Lemma 3.1 of [432].

We are now in position to prove the very useful *product formula*.

Lemma B.2. *Let k be an algebraic number field and α a non-zero element of k. Then,*

$$\prod_{v \in M_k} |\alpha|_v^{d_v} = 1.$$

Proof. This formula is true for $k = \mathbb{Q}$. The lemma then follows from (B.2) and (B.4). □

Theorem B.3. *Let k be an algebraic number field and α in k. Let K be a finite extension of k. Let M_k (resp., M_K) be the set of places on k (resp., on K) and d_v (resp., D_v) the local degree at the place v of M_k (resp., of M_K). Then,*

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} D_v \log \max\{1, |\alpha|_v\} = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} d_v \log \max\{1, |\alpha|_v\}.$$

Proof. It is sufficient to show that for each place v in M_k we have

$$\sum_{w|v} D_w = [K:k] d_v,$$

where the sum is taken over the places w of K which divide v. Let γ be in K such that $K = \mathbb{Q}(\gamma)$. Note that $K = k(\gamma)$. The irreducible polynomial $g(X)$ of γ over k, which is of degree $[K:k]$, factors into irreducible polynomials in $k_v[X]$: let us write $g(X) = \prod_{w|v} g_w(X)$, where g_w is of degree $[K_w : k_v]$. Therefore, for each v in M_k, we have

$$\sum_{w|v} [K_w : k_v] = [K:k].$$

Since $D_w = [K_w : k_v] d_v$, our claim follows. □

We immediately get from Theorem B.3 that the following definition of the (logarithmic) Weil height of an algebraic number does not depend on the number field in which it is contained.

Definition B.4. Let α be a complex algebraic number in a number field k. The (logarithmic) Weil height of α is

$$h(\alpha) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} d_v \log \max\{1, |\alpha|_v\}, \tag{B.5}$$

where d_v denotes the local degree at the place v of M_k.

It follows from the definition of the height that, if a and b are coprime non-zero integers, then

$$h\Big(\frac{a}{b}\Big) = \log \max\{|a|, |b|\}$$

and, if a and d are positive integers, then

$$h(\sqrt[d]{a}) = \frac{\log a}{d}.$$

Theorem B.5. *For all algebraic numbers α_1 and α_2, we have*

$$h(\alpha_1\alpha_2) \le h(\alpha_1) + h(\alpha_2)$$

and

$$h(\alpha_1 + \alpha_2) \le \log 2 + h(\alpha_1) + h(\alpha_2).$$

Furthermore, for any non-zero algebraic number α and any integer n, we have

$$h(\alpha^n) = |n| h(\alpha). \tag{B.6}$$

Proof. The first inequalities follow from Definition B.4 and the upper bounds

$$\max\{1, xy\} \le \max\{1, x\} \max\{1, y\}, \qquad \text{for all } x \ge 0,\ y \ge 0,$$

and

$$\max\{1, x + y\} \le 2 \max\{1, x\} \max\{1, y\}, \qquad \text{for all } x \ge 0,\ y \ge 0.$$

In view of (B.5), it is sufficient to establish (B.6) for $n = -1$. Let d denote the degree of α, set $k = \mathbb{Q}(\alpha)$, and, for v in M_k, let d_v denote the local degree at the place v. It follows from Lemma B.2 that

$$\frac{1}{d} \sum_{\substack{v \in M_k, \\ |\alpha|_v \ge 1}} d_v \log |\alpha|_v = \frac{1}{d} \sum_{\substack{v \in M_k, \\ |\alpha|_v \le 1}} d_v \log \frac{1}{|\alpha|_v}.$$

The left hand side of the above equality is equal to $h(\alpha)$, while the right hand side is equal to $h(\alpha^{-1})$. Thus, we get $h(\alpha) = h(\alpha^{-1})$. □

The next statement characterises the algebraic numbers whose height is equal to zero. It is often referred to as Kronecker's theorem [245].

Theorem B.6. *The only non-zero algebraic numbers of height equal to zero are the roots of unity.*

Proof. Let α be a non-zero algebraic number of height equal to zero. Then, we have $|\alpha|_v \le 1$ for every place v of $\mathbb{Q}(\alpha)$. Let d denote the degree of α and $a_d X^d + \cdots + a_1 X + a_0$ its minimal defining polynomial over $\mathbb{Z}$. Let p be a prime number. For $j = 0, \ldots, d-1$, expressing $\frac{a_j}{a_d}$ as a symmetric function of the Galois conjugates of α and using that the p-adic absolute value is ultrametric, we deduce that $|a_j|_p \le |a_d|_p$. Since $a_0, \dots, a_d$ are relatively prime, we get that $|a_d|_p = 1$ and conclude that α is an algebraic integer.

Let ℓ be a positive integer. All the Galois conjugates of α^ℓ have modulus at most equal to one. Consequently, α^ℓ is a root of a monic integer polynomial of degree d and whose coefficients are in absolute value bounded from above by 2^d. Since the set of such polynomials is finite, there exist distinct positive integers ℓ and ℓ' such that $\alpha^\ell = \alpha^{\ell'}$. We conclude that α is a root of unity. □

We conclude this section with a result often referred to as Northcott's theorem [317].

Theorem B.7. *There are only finitely many algebraic numbers of bounded degree and bounded height.*

Proof. Let α be an algebraic number of degree at most d and height at most H. Then, the leading coefficient a of the minimal defining polynomial $P_\alpha(X)$ of α over the integers and all the Galois conjugates of α are bounded in absolute value in terms of d and H. By expressing the coefficients of $P_\alpha(X)$ in terms of a and the symmetric functions of the Galois conjugates of α, we see that they are all bounded in absolute value in terms of d and H. Consequently, the set of algebraic numbers of degree at most d and height at most H is finite. □

B.2. The Liouville inequality

By "Liouville's inequality", we mean a non-trivial lower bound for the value of a polynomial with integer (or algebraic) coefficients evaluated at a tuple of algebraic numbers (when this value is non-zero), and expressed in terms of the degrees and the heights of the polynomial and of the algebraic numbers involved. A typical example is given by Theorem A.5.

One of the most useful inequalities of Liouville's type is the following one.

Theorem B.8. *For every non-zero algebraic number α of degree d and every place v of $M_{\mathbb{Q}(\alpha)}$ of local degree d_v, we have*

$$d_v \log |\alpha|_v \ge -dh(\alpha). \tag{B.7}$$

In particular, we get $\mathrm{v}_p(\alpha) \log p \le dh(\alpha)$ for every prime number p.

Proof. By the definition of the height of α^{-1}, we have

$$d_v \log |\alpha^{-1}|_v \le [\mathbb{Q}(\alpha^{-1}) : \mathbb{Q}] h(\alpha^{-1}).$$

Since $h(\alpha) = h(\alpha^{-1})$ and $[\mathbb{Q}(\alpha^{-1}) : \mathbb{Q}] = d$, this gives (B.7). □

Definition B.9. The length $\mathrm{L}(f)$ of the polynomial $f(X_1, \dots, X_t)$ in t variables and with complex coefficients is the sum of the moduli of its coefficients.

We can now state a version of Liouville's inequality (for a sharper version, with the L^1-norm in place of the length, see Exercise 3.2 of [432]).

Theorem B.10. *Let $f(\mathrm{X}_1, \dots, \mathrm{X}_t)$ be a non-zero polynomial in t variables with integer coefficients. Let $\gamma_1, \dots, \gamma_t$ be algebraic numbers in an algebraic number field K of degree d. Then*

$$h\big(f(\gamma_1, \dots, \gamma_t)\big) \le \log \mathrm{L}(f) + \sum_{i=1}^{t} (\deg_{\mathrm{X}_i} f) h(\gamma_i) \tag{B.8}$$

and, for every place v of K,

$$\log |f(\gamma_1, \dots, \gamma_t)|_v \ge -\frac{d}{d_v} \Big(\log \mathrm{L}(f) + \sum_{i=1}^{t} (\deg_{\mathrm{X}_i} f) h(\gamma_i)\Big), \tag{B.9}$$

where d_v denotes the local degree at the place v.

Proof. Let v be a place of K. If v is non-Archimedean, then

$$\log \max\{1, |f(\gamma_1, \dots, \gamma_t)|_v\} \le \sum_{i=1}^{\ell} (\deg_{\mathrm{X}_i} f) \log \max\{1, |\gamma_i|_v\}.$$

If v is Archimedean, then

$$\log \max\{1, |f(\gamma_1, \dots, \gamma_t)|_v\} \le \log \mathrm{L}(f) + \sum_{i=1}^{\ell} (\deg_{\mathrm{X}_i} f) \log \max\{1, |\gamma_i|_v\}.$$

Since the sum of the local degrees over all the Archimedean places is equal d, we easily deduce (B.8) and, by applying (B.7), we get (B.9). □

B.3. Linear forms in one p-adic logarithm

The next statement is an explicit version of Lemma A.8 from [376]; see also Lemma 1.4 of [444].

Theorem B.11. *Let p be a prime number, $m \ge 2$ an integer, and α an algebraic number of degree d such that α^m is not equal to 1. Then, we have*

$$\mathrm{v}_p(\alpha^m - 1) \le \frac{\log m}{\log p} + 2d \frac{p^d - 1}{\log p} h(\alpha) + 2d \frac{\log 2}{\log p}. \tag{B.10}$$

Proof. If α is a root of unity, then so is α^m and the height of $\alpha^m - 1$ is, by Theorem B.5, bounded from above by $\log 2$. The upper bound (B.10) follows from Theorem B.8. We can assume that α is not a root of unity and that $\mathrm{v}_p(\alpha^m - 1)$ is positive. This implies that $\mathrm{v}_p(\alpha) = 0$. Let s be the smallest positive integer such that $\mathrm{v}_p(\alpha^s - 1)$ is positive. By Lemma F.4, it satisfies $s \le p^d - 1$. Since

$$\mathrm{v}_p(\alpha^m - 1) \le \mathrm{v}_p((\alpha^s)^m - 1),$$

we may assume that $\mathrm{v}_p(\alpha - 1) = 0$. Setting

$$m = p^a m', \quad \gcd(p, m') = 1, \quad \beta = \alpha^{p^a},$$

we get

$$\alpha^m - 1 = \Big(\frac{\beta^{m'} - 1}{\beta - 1}\Big)\Big(\frac{\beta - 1}{\alpha - 1}\Big)(\alpha - 1).$$

Since p does not divide m' and $\mathrm{v}_p(\beta - 1) > 0$, we obtain that

$$\mathrm{v}_p\Big(\frac{\beta^{m'} - 1}{\beta - 1}\Big) = \mathrm{v}_p(1 + \beta + \cdots + \beta^{m'-1}) = 0.$$

Furthermore, since $\mathrm{v}_p(\alpha - 1) > 0$, we get

$$\mathrm{v}_p\Big(\frac{\beta - 1}{\alpha - 1}\Big) \le a + \mathrm{v}_p(\alpha + 1) \le \frac{\log m}{\log p} + \mathrm{v}_p(\alpha + 1).$$

By Theorems B.8 and B.5, we have

$$\mathrm{v}_p(\alpha \pm 1)\ \log p \le d h(\alpha \pm 1) \le d(h(\alpha) + \log 2).$$

This completes the proof of the theorem. □

Appendix C
Auxiliary results on algebraic number fields

In a first section, we display without proofs classical results on Pellian equations. The second section is devoted to results from algebraic number theory, which are very useful for the effective resolution of classical families of Diophantine equations.

C.1. Real quadratic fields and Pellian equations

Classical references include Nagell's book [312] and LeVeque's monograph [260]; see also [11]. We omit the proofs. Equation (C.1) below is usually called the Pell equation.

THEOREM C.1. *Let D be a positive integer which is not a perfect square. Then, the Diophantine equation*

$$x^2 - Dy^2 = 1 \tag{C.1}$$

has infinitely many solutions in integers x, y. Furthermore, all the solutions to (C.1) in positive integers x, y are given by the formula

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n, \quad n \ge 1, \tag{C.2}$$

where $x_1 + y_1\sqrt{D}$ is the fundamental solution of (C.1), that is, the solution with the smallest positive x.

It follows from (C.1) and (C.2) that the integer sequences $(x_n)_{n\ge1}$ and $(y_n)_{n\ge1}$ satisfy the same linear recurrence relation, namely

$$Z_{n+1} = 2x_1 Z_n - Z_{n-1}, \quad n \ge 2.$$

If in (C.1) the right hand side 1 is replaced by a non-zero integer N, then the corresponding equation $x^2 - Dy^2 = N$ has either no solutions (consider, for example, the equation $x^2 - 3y^2 = -1$ and argue modulo 4), or infinitely many solutions. In the latter case, the set of solutions can be precisely described. Equations (C.3) below are usually called Pellian equations.

THEOREM C.2. *If D and N are positive integers and D is not a perfect square, then the Diophantine equations*

$$x^2 - Dy^2 = N \quad \text{and} \quad x^2 - Dy^2 = -N \tag{C.3}$$

have a finite number of classes of solutions. If $x^* + y^*\sqrt{D}$ denotes the fundamental solution of a given class (that is, the solution with minimal positive x^*), then all the solutions in this class are obtained by the formula

$$x_n^* + y_n^*\sqrt{D} = (x^* + y^*\sqrt{D})(x + y\sqrt{D}),$$

where (x, y) runs through the set of solutions of (C.1).

Finally, we define the fundamental unit of a real quadratic field.

Definition C.3. Let D be a squarefree integer with $D \geq 2$. Let (t, u) be the solution with smallest positive t and $u \geq 1$ to the equation

$$x^2 - Dy^2 = \pm 4.$$

Then, setting $x_1 := \frac{t}{2}$, $y_1 := \frac{u}{2}$, the unit $\eta := x_1 + y_1\sqrt{D}$ is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{D})$, that is, η is greater than 1 and all the units of $\mathbb{Q}(\sqrt{D})$ are of the form $\pm\eta^m$, for some rational integer m.

It is not difficult to check that the smallest fundamental unit of a real quadratic field is the Golden Ratio $(1 + \sqrt{5})/2$.

C.2. Algebraic number fields

We gather in this section several classical results and four auxiliary statements on algebraic number fields, which are used when applying linear forms in logarithms to derive effective upper bounds for the size of the solutions to classical families of Diophantine equations, including S-unit equations, Thue equations, superelliptic equations, etc. We omit most of the proofs. The reader is directed to Chapter A of [376], the monograph of Narkiewicz [315], and Chapter 1 of [182].

Let K be an algebraic number field of degree d. Let denote by O_K its ring of integers and by D_K its discriminant. Let S be a finite set of places of K containing all the infinite places and s denote its cardinality. Let $v_1, \ldots, v_{s-1}$ be a subset of S and $\{\eta_1, \ldots, \eta_{s-1}\}$ a fundamental system of S-units in K (that is, every S-unit in K can be written uniquely as the product of a root of unity in K times $\eta_1^{b_1} \cdots \eta_{s-1}^{b_{s-1}}$, for some integers $b_1, \ldots, b_{s-1}$). Denote by R_S the absolute value of the determinant of the matrix $(\log|\eta_i|_{v_j}^{d_j})_{i,j=1,\ldots,s-1}$, where d_j denotes the local degree at the place v_j. It is easy to check that R_S is positive and independent of the choice of $v_1, \ldots, v_{s-1}$ and of the fundamental system of S-units $\{\eta_1, \ldots, \eta_{s-1}\}$. It is called the S-regulator of K. If S is the set of infinite places of K, then R_S is the regulator of K.

Lemma C.4. *Keep the above notation. If S is the set of infinite places of K, then put $P = \mathrm{e}$; otherwise, let P denote the largest prime number lying below a finite place of S. There exists a fundamental system $\{\eta_1, \ldots, \eta_{s-1}\}$ of S-units in K such that*

$$\prod_{i=1}^{s-1} h(\eta_i) \ll_{d,s} R_S \ll_{d,D_K,s} (\log P)^s,$$

$$h(\eta_i) \ll_{d,s} R_S \ll_{d,D_K,s} (\log P)^s, \quad i = 1, \ldots, s-1,$$

and the absolute values of the entries of the inverse matrix of $(\log|\eta_i|_{v_j}^{d_j})_{i,j=1,\ldots,s-1}$ are $\ll_{d,s} 1$.

Proof. This follows from Lemma 3 in [124]; see also Proposition 4.3.9 of [182]. □

Proposition C.5. *Keep the above notation with S being the set of infinite places of K. Let r denote the unit rank of K. Let n be a positive integer. Then, for every non-zero algebraic integer β in K, there exist integers $b_1, \ldots, b_r$ such that, setting $\mu = \beta \eta_1^{-nb_1} \cdots \eta_r^{-nb_r}$ and $B = \max\{|b_1|, \ldots, |b_r|\}$, we have*

$$\left| h(\mu) - \frac{\log |\operatorname{Norm}_{K/\mathbb{Q}}(\beta)|}{d} \right| \ll_{d, D_K, n} 1$$

and

$$B \ll_{d, D_K} \max\{h(\beta), 1\}.$$

Proof. This is Lemma 2 in [124]; see also Proposition 4.3.12 of [182]. □

Proposition C.5 asserts that, for any given algebraic integer β in K, there exists a unit η in K such that the height of $\eta\beta$ is controlled in terms of the degree and the discriminant of K and in terms of the norm of β. Said differently, in any integer ideal, there exists an algebraic number of small height.

The next proposition is a key ingredient in the proofs of Theorems 4.7 and 4.9.

Proposition C.6. *Let $f(X)$ be a monic integer polynomial without multiple roots and of degree at least equal to 2. Let K denote the splitting field of $f(X)$ and h_K its class number. Let n be an integer with $n \geq 2$. Let t be a non-zero integer. Let x and y be integers satisfying*

$$f(x) = ty^n.$$

Let α be a root of $f(X)$. Then, there are algebraic integers β, γ, δ in K such that

$$\delta(x - \alpha) = \beta\gamma^n \quad \text{and} \quad h(\beta), h(\delta) \ll_{f,t,n} 1.$$

Furthermore, there are algebraic integers $\beta_1, \gamma_1, \delta_1$ in K and a unit ζ_1 in K such that

$$\delta_1(x - \alpha)^{h_K} = \zeta_1 \beta_1 \gamma_1^n \quad \text{and} \quad h(\beta_1), h(\delta_1) \ll_{f,t} 1. \tag{C.4}$$

We stress that the upper bounds for the heights of β_1 and δ_1 in (C.4) do not depend on n.

Proof. The first assertion is Lemma 6.1 in [376] and the second one is established on page 22 of [95]. Their proofs can be summarized as follows. Assume that $x \neq \alpha$ and let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_m$ be the roots of $f(X)$. The greatest common divisor of the principal ideals $(x - \alpha)O_K$ and $(x - \alpha_2) \ldots (x - \alpha_m)O_K$ divides the ideal $f'(\alpha)O_K$. Since $\operatorname{Norm}_{K/\mathbb{Q}}\big(f'(\alpha)\big)$ divides the discriminant of $f(X)$, there exist integral ideals $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ of O_K such that

$$\mathfrak{a}\,(x - \alpha)O_K = \mathfrak{b}\,\mathfrak{c}^n \tag{C.5}$$

and

$$\operatorname{Norm}_{K/\mathbb{Q}}(\mathfrak{a}) \ll_{f,t} 1, \quad \operatorname{Norm}_{K/\mathbb{Q}}(\mathfrak{b}) \ll_{f,t} 1.$$

Then, we apply a theorem of Minkowski (see Theorem A.1 and Lemma A.11 in [376]) to deduce the existence of integral ideals $\mathfrak{b}'$, $\mathfrak{c}'$ in O_K whose norms over $\mathbb{Q}$ are $\ll_{f,t} 1$ and which are such that the ideals $\mathfrak{b}\mathfrak{b}'$ and $\mathfrak{c}\mathfrak{c}'$ are principal. By multiplying both sides of (C.5) by $\mathfrak{b}'(\mathfrak{c}')^n$, we deduce that the ideal $\mathfrak{a}\mathfrak{b}'(\mathfrak{c}')^n$ is principal. Furthermore, its norm over $\mathbb{Q}$ is $\ll_{f,t,n} 1$. The first assertion of the lemma then follows from Proposition C.5. For the second assertion we raise (C.5) to the power h_K and recall that the h_K-th power of any integral ideal in O_K is principal. Then, we again apply Proposition C.5 to conclude. □

Lemma C.7. *Let K be a number field and L a finite extension of K. Let α be such that $L = K(\alpha)$. Then, the absolute value of the discriminant of L is bounded from above in terms of the degree and discriminant of K and of the degree and height of α.*

Proof. This follows from Corollary A.7 of [376]. □

Appendix D
Classical results on prime numbers

We denote by $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ the increasing sequence of prime numbers. In this short appendix, we recall several useful results on prime numbers and arithmetical functions, most of which are proved in [220].

We begin with Bertrand's postulate [220, Theorem 418].

Theorem D.1. *For every integer k with $k \geq 2$, there exists at least one prime number p satisfying $k < p < 2k$.*

We continue with the Prime number theorem [220, Theorem 8] and two of its immediate consequences.

Theorem D.2. *We have*

$$\lim_{t \to +\infty} \frac{p_t}{t \log t} = 1, \quad \lim_{t \to +\infty} \frac{\sum_{j=1}^{t} \log p_j}{t \log t} = 1, \quad \textit{and} \quad \lim_{t \to +\infty} \frac{\sum_{j=1}^{t} \log \log p_j}{t \log \log t} = 1.$$

In the course of the present book, three classical arithmetical functions appear naturally. We recall their definitions and some of their properties.

Definition D.3. Let $n \geq 2$ be an integer. We denote by $\omega(n)$ the total number of distinct prime factors of n and by $\varphi(n)$ the number of positive integers less than n and coprime to n. The function φ is called the Euler totient function. The Möbius function μ is defined by $\mu(n) = 0$ if the integer n is divisible by the square of a prime number, and $\mu(q_1 \cdots q_k) = (-1)^k$ if the prime numbers $q_1, \ldots, q_k$ are distinct. Furthermore, we set $\omega(1) = 0, \varphi(1) = 1$, and $\mu(1) = 1$.

We begin with an upper bound for the function ω.

Theorem D.4. *For every integer $n \geq 3$ we have*

$$\omega(n) \ll \frac{\log n}{\log \log n}.$$

Proof. The number of distinct prime factors of n is at most equal to the integer k defined by the inequalities

$$\prod_{j=1}^{k} p_j \leq n < \prod_{i=1}^{k+1} p_j.$$

It follows from Theorem D.2 that

$$k \log k \ll \log n,$$

and the theorem follows. □

Theorem D.5. *There exists a real number C such that, for every integer $n \geq 3$, we have*

$$\varphi(n) \geq \frac{n}{(\log\log n)^C}.$$

Proof. Observe that

$$\varphi(n) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big), \tag{D.1}$$

where the product is taken over all the distinct prime divisors of n. We estimate

$$\log \frac{\varphi(n)}{n} \geq \sum_{j=1}^{\omega(n)} \log\Big(1 - \frac{1}{p_j}\Big) \gg \Big(-\sum_{j=1}^{\omega(n)} \frac{1}{j\log(2j)}\Big) \gg \big(-\log\log\omega(n)\big). \tag{D.2}$$

We deduce from (D.2) and Theorem D.4 that there exist real numbers c_1 and c_2 such that

$$\frac{\varphi(n)}{n} \geq (\log\omega(n))^{-c_1} \geq (\log\log n)^{-c_2}.$$

This proves the theorem. □

Much more is known on the Euler totient function, namely (see Theorem 328 of [220]) that it satisfies

$$\liminf_{n\to+\infty} \frac{\varphi(n)\log\log n}{n} = \mathrm{e}^{-\gamma}, \tag{D.3}$$

where

$$\gamma := \lim_{n\to+\infty} \Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\Big)$$

is the Euler constant. It is possible to deduce from Theorem D.2 that the lim inf in (D.3) is positive; see [220].

The next result establishes a relation between the Euler totient function and the Möbius function.

Theorem D.6. *For any integer $n \geq 2$, we have*

$$\varphi(n) = \sum_{m|n} m\,\mu\Big(\frac{n}{m}\Big) \quad \textit{and} \quad \sum_{m|n} \mu(m) = 0.$$

Proof. It follows from (D.1), the definition of the Möbius function, and a change of variables that

$$\varphi(n) = n\sum_{m|n} \frac{\mu(m)}{m} = \sum_{m|n} m\,\mu\Big(\frac{n}{m}\Big).$$

Furthermore, if $q_1, \ldots, q_k$ denote the prime divisors of n, then

$$0 = \big(1 + (-1)\big)^k = \sum_{m|q_1\cdots q_k} \mu(m) = \sum_{m|n} \mu(m).$$

This completes the proof of the theorem. □

The last result is much less classical.

THEOREM D.7. *Let x and n be integers with $3 \leq n < x$. The number of prime numbers which are not greater than x and congruent to ± 1 modulo n does not exceed $\frac{6x}{\varphi(n)\log(x/n)}$.*

Proof. This follows from a version of the Brun–Titchmarsch theorem; see Theorem 3.8 of [218]. □

Appendix E
A zero lemma

Most of the proofs in transcendence theory go as follows, an emblematic example being given by the proof of Theorem A.5. We define a suitable quantity as a combination of algebraic numbers. We bound its absolute value from above by means of analytic tools and from below by using the Liouville inequality. We reach a contradiction when the lower bound exceeds the upper bound. But we need also to prove that our quantity is not zero, which is often a very delicate part of the proof. To do this step, we require so-called zero lemmas.

In this appendix, we establish a zero lemma for polynomials in two variables.

Lemma E.1. *Let $\alpha_1, \alpha_2, b_1, b_2$ be complex numbers with $\alpha_1\alpha_2 \neq 0$. Let K, L be positive integers and $\mathcal{E}, \mathcal{E}'$ finite subsets of $\mathbb{Z}^2$. Let $P(X, Y)$ be a non-zero complex polynomial of degree at most $K-1$ in X and degree at most $L-1$ in Y. Assume that*

$$\operatorname{Card}\bigl\{\alpha_1^r\,\alpha_2^s : (r,s) \in \mathcal{E}\bigr\} \ge L \tag{E.1}$$

and

$$\operatorname{Card}\bigl\{b_2 r' + b_1 s' : (r',s') \in \mathcal{E}'\bigr\} > (K-1)\,L. \tag{E.2}$$

Then, at least one of the numbers

$$P\bigl(b_2(r+r') + b_1(s+s'), \alpha_1^{r+r'}\,\alpha_2^{s+s'}\bigr), \quad (r,s) \in \mathcal{E}, \quad (r',s') \in \mathcal{E}', \tag{E.3}$$

is non-zero.

Lemma E.1 is close to be best possible. Before proving it, we state an auxiliary result.

Lemma E.2. *Let n be a positive integer and $K_1, \ldots, K_n, L$ integers with*

$$0 \le K_1 < K_2 < \cdots < K_n < L.$$

Let $\mathcal{E}$ be a set of at least L complex numbers. There exist $a_1, \ldots, a_n$ in $\mathcal{E}$ such that the determinant of the matrix $(a_j^{K_i})_{1 \le i,j \le n}$ is non-zero.

Proof. We proceed by induction on n. The case $n = 1$ is immediate. Let $n \ge 2$ be an integer and assume that the lemma holds for $n-1$. Let $K_1, \ldots, K_n, L$ be integers with $0 \le K_1 < K_2 < \cdots < K_n < L$. By the induction hypothesis, there exist $a_1, \ldots, a_{n-1}$

in $\mathscr{E}$ such that the determinant A of the matrix $(a_j^{K_i})_{1\le i,j\le n-1}$ is non-zero. Then, the polynomial

$$P(z) := \det \begin{pmatrix} a_1^{K_1} & \cdots & a_{n-1}^{K_1} & z^{K_1} \\ a_1^{K_2} & \cdots & a_{n-1}^{K_2} & z^{K_2} \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{K_n} & \cdots & a_{n-1}^{K_n} & z^{K_n} \end{pmatrix} = Az^{K_n} + \cdots$$

is of degree K_n and it can be written as $P(z) = (z-a_1)\cdots(z-a_{n-1})Q(z)$, for a complex polynomial $Q(z)$. Since the set $\mathscr{E} \setminus \{a_1, \ldots, a_{n-1}\}$ contains at least

$$L - (n-1) > K_n - (n-1) = \deg Q$$

elements, there exists a_n in $\mathscr{E} \setminus \{a_1, \ldots, a_{n-1}\}$ such that $Q(a_n)$ is non-zero. Thus, $P(a_n)$ is non-zero as well. □

Proof of Lemma E.1. Without any loss of generality, we assume that Y does not divide $P(X,Y)$. Assume that all the numbers in (E.3) are zero. Define the integers $K_1 = 0 < K_2 < \cdots < K_n < L$ by writing $P(X,Y)$ as a polynomial in Y with coefficients in $\mathbb{C}[X]$:

$$P(X,Y) = \sum_{i=1}^{n} Q_i(X)Y^{K_i}, \quad Q_i(X) \neq 0, \quad i = 1, \ldots, n.$$

By (E.1) and Lemma E.2, there exists a subset $\mathscr{L}$ of $\mathscr{E}$ of cardinality n such that

$$B := \det((\alpha_1^r \alpha_2^s)^{K_i})_{1\le i\le n,(r,s)\in\mathscr{L}} \neq 0.$$

For (r,s) in $\mathscr{L}$, consider the polynomial

$$\begin{aligned} P_{r,s}(X,Y) &:= P(X + b_2 r + b_1 s, \alpha_1^r \alpha_2^s Y) \\ &= \sum_{i=1}^{n} Q_i(X + b_2 r + b_1 s)(\alpha_1^r \alpha_2^s)^{K_i}\, Y^{K_i}, \end{aligned} \tag{E.4}$$

and set

$$\Delta(X) = \det\bigl(Q_i(X + b_2 r + b_1 s)(\alpha_1^r \alpha_2^s)^{K_i}\bigr)_{1\le i\le n,\,(r,s)\in\mathscr{L}}.$$

For $i = 1, \ldots, n$, write $Q_i(X) = q_i X^{m_i} + \cdots$ with $q_i \neq 0$ and observe that

$$\Delta(X) = q_1 \cdots q_n B X^{m_1+\cdots+m_n} + \cdots$$

with $q_1 \ldots q_n B \neq 0$. Viewing (E.4) as a linear system of n equations in the n variables $Y^{K_1}, \ldots, Y^{K_n}$, there exist, by Cramer's rule, polynomials $S_{r,s}(X)$ in $\mathbb{C}[X]$, indexed by (r,s) in $\mathscr{L}$, such that

$$Y^{K_1}\Delta(X) = \Delta(X) = \sum_{(r,s)\in\mathscr{L}} P_{r,s}(X,Y) \cdot S_{r,s}(X).$$

By assumption, we have

$$P_{r,s}(b_2r' + b_1s', \alpha_1^{r'}\alpha_2^{s'}) = 0, \quad (r,s) \in \mathcal{L}, \quad (r',s') \in \mathcal{E}'.$$

It then follows that $\Delta(b_2r' + b_1s') = 0$ for (r',s') in $\mathcal{E}'$ and, by (E.2), the non-zero polynomial $\Delta(X)$ has more than $(K-1)L$ roots. Hence, we get

$$(K-1)L < \deg \Delta = m_1 + \cdots + m_n \leq n(K-1) \leq (K-1)L.$$

This contradiction proves the lemma. □

Appendix F
Tools from complex and p-adic analysis

In this appendix, we gather auxiliary results from complex and p-adic analysis used to establish lower bounds for linear forms in two complex and p-adic logarithms.

F.1. The Schwarz lemma in complex analysis

We need only a basic version of Schwarz' lemma, namely for analytic functions of a single variable with a single (multiple) zero. For a positive real number R and a function f analytic in the closed disc centered at 0 and of radius R, we denote by $|f|_R$ the maximum of $|f(z)|$, where z runs over this disc. Obviously, if r satisfies $0 < r < R$, then $|f|_r \leq |f|_R$. The purpose of the Schwarz lemma is to improve this inequality when f has many zeros, counted with multiplicity, in the closed disc centered at 0 and of radius r.

Lemma F.1. *Let T be a non-negative integer, r and R real numbers satisfying $0 < r \leq R$, and Ψ a function of one complex variable which is analytic in the closed disc centered at the origin and of radius R. Assume that Ψ has a zero of multiplicity at least T at 0. Then*

$$|\Psi|_r \leq \left(\frac{R}{r}\right)^{-T} |\Psi|_R.$$

Proof. The function $z \mapsto \Phi(z) := z^{-T}\Psi(z)$ is analytic in the disc $\{z : |z| \leq R\}$. It follows from the maximum modulus principle that

$$|\Phi|_r = r^{-T}|\Psi|_r \quad \text{and} \quad |\Phi|_R = R^{-T}|\Psi|_R. \tag{F.1}$$

Since $r \leq R$, we have $|\Phi|_r \leq |\Phi|_R$. Combined with (F.1), this proves the lemma. □

F.2. Auxiliary results on p-adic fields

Throughout this section, p denotes a prime number and K a finite extension of $\mathbb{Q}_p$. We state below several elementary or classical results.

Let e be the ramification index of K and f its residue degree (see Appendix B for the definitions).

Lemma F.2. *Let θ be in K such that $\mathrm{v}_p(\theta - 1) > 0$. Then*

$$\mathrm{v}_p(\theta^p - 1) = p\mathrm{v}_p(\theta - 1), \qquad \textit{if } \mathrm{v}_p(\theta - 1) < \frac{1}{p-1},$$

$$\begin{aligned} \mathrm{v}_p(\theta^p-1) &= \mathrm{v}_p(\theta-1)+1, && \textit{if } \mathrm{v}_p(\theta-1) > \frac{1}{p-1},\\ \mathrm{v}_p(\theta^p-1) &\geq \frac{p}{p-1} = \frac{1}{p-1}+1, && \textit{if } \mathrm{v}_p(\theta-1) = \frac{1}{p-1}. \end{aligned}$$

Proof. It follows from the binomial identity

$$x^p-1 = (x-1)^p + \sum_{j=1}^{p-1} \frac{p}{j}\binom{p-1}{j-1}(x-1)^j$$

that

$$\mathrm{v}_p\left(\theta^p-1\right) \geq \min\left\{p\mathrm{v}_p(\theta-1), 1+\mathrm{v}_p(\theta-1)\right\},$$

with equality if the two terms in the minimum are distinct. Observe that these two terms are equal when $\mathrm{v}_p(\theta-1) = \frac{1}{p-1}$. The assertions of the lemma then follow. □

Lemma F.3. *Let θ be in K such that $\mathrm{v}_p(\theta-1) > 0$. Let $t \geq 0$ be the integer satisfying the inequalities*

$$p^{t-1} \leq \frac{3e}{2(p-1)} < p^t.$$

Then

$$\mathrm{v}_p\left(\theta^{p^t}-1\right) > \frac{p^t}{3e} + \frac{1}{p-1}.$$

Proof. The conclusion of the lemma holds if $\mathrm{v}_p(\theta-1) > \frac{p}{p-1}$, since $\frac{p^t}{3e} \leq \frac{p}{2(p-1)} \leq 1$. Thus, we assume that $\mathrm{v}_p(\theta-1) \leq \frac{p}{p-1}$. Let u be the greatest integer less than or equal to t such that $p^{u-1}\mathrm{v}_p(\theta-1) \leq \frac{1}{p-1}$. Then, by induction and using Lemma F.2, we get

$$\mathrm{v}_p\left(\theta^{p^u}-1\right) \geq p^u\mathrm{v}_p(\theta-1)$$

and

$$\mathrm{v}_p\left(\theta^{p^t}-1\right) \geq p^u\mathrm{v}_p(\theta-1) + (t-u). \tag{F.2}$$

If $u=t$, then the inequality $\mathrm{v}_p(\theta-1) \geq \frac{1}{e}$ and (F.2) imply that

$$\mathrm{v}_p\left(\theta^{p^t}-1\right) \geq \frac{p^t}{e} = \frac{p^t}{3e} + \frac{2p^t}{3e} > \frac{p^t}{3e} + \frac{1}{p-1}.$$

If $u<t$, then $p^u\mathrm{v}_p(\theta-1) > \frac{1}{p-1}$ and we deduce from (F.2) that

$$\mathrm{v}_p\left(\theta^{p^t}-1\right) > \frac{1}{p-1} + 1 \geq \frac{1}{p-1} + \frac{p^t}{3e},$$

since $\frac{p^t}{3e} \leq \frac{p}{2(p-1)} \leq 1$. This completes the proof of the lemma. □

We further need classical properties of p-adic fields. A good reference is the monograph of Robert [347]. Let U (*resp.,* U^1) denote the (multiplicative) group of units (*resp.,* of principal units, that is, of units θ such that $\mathrm{v}_p(\theta - 1) > 0$) of K.

Lemma F.4. *The quotient group U/U^1 is cyclic of cardinality $p^f - 1$ and each class contains a unique $(p^f - 1)$-th root of unity.*

Proof. This is Proposition 8 of Chapter 2 of [365]. □

Lemma F.5. *Let u be a positive integer. For any root of unity ζ of order p^u, the ramification index of the extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is equal to $p^{u-1}(p-1)$. Furthermore, for any positive integer m not divisible by p, we have*

$$\sum_{\substack{\zeta^{mp^u}=1 \\ \zeta\neq 1}} \mathrm{v}_p(\zeta - 1) = u.$$

Proof. The first assertion and the case $m = 1$ of the second one follow from the theorem on page 107 of [347]. For $m \geq 2$, see Proposition 17 of Chapter 4 of [365]. □

Lemma F.6 (Krasner's lemma). *Let ξ and ξ' be in an algebraic closure of $\mathbb{Q}_p$. Let $\xi_1 := \xi, \xi_2, \dots, \xi_d$ denote the Galois conjugates of ξ over $\mathbb{Q}_p$. If*

$$\mathrm{v}_p(\xi' - \xi) > \mathrm{v}_p(\xi' - \xi_i), \quad i = 2, \dots, d,$$

then ξ is an element of the field $\mathbb{Q}_p(\xi')$.

Proof. See e.g. [347, p. 130]. □

F.3. The Schwarz lemma in p-adic analysis

Let p be a prime number. We start this section by recalling informally some classical results in p-adic analysis. Good references include [203, 242, 347, 351] and Chapter 17 of [223].

The p-adic logarithm function $\log_p$ is defined in the open disc $B(1,1)$ of $\mathbb{C}_p$ centered at 1 and of radius 1 by the series

$$\log_p(x) = \log_p\bigl(1 + (x-1)\bigr) = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

and is analytic in $B(1,1)$. Furthermore, every x in $B(1,1)$ satisfies $\mathrm{v}_p(\log_p(x)) = \mathrm{v}_p(x-1)$.

The p-adic exponential function $\exp_p$ is defined in the open disc of $\mathbb{C}_p$ centered at the origin and of radius $p^{-1/(p-1)}$ by the series

$$\exp_p(x) = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

and is analytic in this disc.

Let a, x be in $\mathbb{C}_p$ with $\mathrm{v}_p(x-1) > \frac{1}{p-1}$ and $\mathrm{v}_p(a) + \mathrm{v}_p(x-1) > \frac{1}{p-1}$. Then, the expression x^a is defined by

$$x^a := \exp_p\bigl(a \log_p(x)\bigr).$$

Lemma F.7. *Let x be in $\mathbb{C}_p$ such that there exists $\theta \geq 0$ with $\mathrm{v}_p(x-1) > \theta + \frac{1}{p-1}$. Then, the function $z \mapsto x^z$ is analytic on the set $\{z \in \mathbb{C}_p : \mathrm{v}_p(z) \geq -\theta\}$.*

Proof. See e.g. Chapter 17 of [223]. □

Let R be a positive real number and $f : z \mapsto \sum_{n \geq 0} a_n z^n$ a formal power series with coefficients in $\mathbb{Q}_p$. Set

$$|f|_R := \sup_{n \geq 0} |a_n|_p R^n. \tag{F.3}$$

We use the same notation as in Section F.1. This should not cause any confusion. If $|f|_R$ is finite, then the series f converges in the disc $\{z \in \mathbb{C}_p : |z|_p < R\}$. It converges in the closed disc $\{z \in \mathbb{C}_p : |z|_p \leq R\}$ when $|a_n|_p R^n$ tends to 0 as n tends to infinity. Moreover, for every z in the disc of convergence of f, we have

$$|f(z)|_p \leq |f|_R.$$

The next statement is a p-adic version of Lemma F.1; see the Appendix of [364].

Lemma F.8. *Let p be a prime number. Let T be a non-negative integer, r and R real numbers satisfying $0 < r \leq R$, and Ψ a power series with coefficients in $\mathbb{Q}_p$ which converges in the closed disc centered at the origin and of radius R. Assume that Ψ has a zero of multiplicity at least T at 0. Then*

$$|\Psi|_r \leq \left(\frac{R}{r}\right)^{-T} |\Psi|_R.$$

Proof. The function $z \mapsto \Phi(z) = z^{-T}\Psi(z)$ is analytic in the disc $\{z \in \mathbb{C}_p : |z| \leq R\}$. We deduce from (F.3) that

$$|\Phi|_r = r^{-T}|\Psi|_r \quad \text{and} \quad |\Phi|_R = R^{-T}|\Psi|_R.$$

Combined with the inequality $|\Phi|_r \leq |\Phi|_R$, this completes the proof. □

Bibliography

[1] M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Théor. Nombres Bordeaux 18 (2006), 299–313. (Cited in Chapter 7.)

[2] A. K. Agrawal, J. H. Coates, D. C. Hunt, and A. J. van der Poorten, *Elliptic curves of conductor 11*, Math. Comp. 35 (1980), 991–1002. (Cited in Chapter 6.)

[3] S. D. Adhikari, N. Saradha, T. N. Shorey, and R. Tijdeman, *Transcendental infinite sums*, Indag Math. 12 (2001), 1–14. (Cited in Chapter 3.)

[4] L. Alaoglu and P. Erdős, *On highly composite and similar numbers*, Trans. Amer. Math. Soc. 56 (1944), 448–469. (Cited in Chapter 13.)

[5] Yu. M. Aleksentsev, *The Hilbert polynomial and linear forms in logarithms of algebraic numbers*, Izv. Ross. Akad. Nauk Ser. Mat. 72 (2008), 6–52 (in Russian); English translation in Izv. Math. 72 (2008), 1063–1110. (Cited in Chapter 2.)

[6] J. Amila, Au balcon d'Hiroshima, Gallimard, 1985.

[7] F. Amoroso, *Algebraic numbers close to* 1 *and variants of Mahler's measure*, J. Number Theory 60 (1996), 80–96. (Cited in Chapter 2.)

[8] F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. 513 (1999), 145–179. (Cited in Chapter 13.)

[9] F. Amoroso and D. Masser, *Lower bounds for the height in Galois extensions*, Bull. Lond. Math. Soc. 48 (2016), 1008–1012. (Cited in Chapter 13.)

[10] F. Amoroso and E. Viada, *Small points on rational subvarieties of tori*, Comment. Math. Helv. 87 (2012), 355–383. (Cited in Chapter 13.)

[11] T. Andreescu and D. Andrica, Quadratic Diophantine equations. Developments in Mathematics, 40. Springer, New York, 2015. (Cited in Appendix C.)

[12] R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1263–1264. (Cited in Chapter 7.)

[13] ———, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1451–1452. (Cited in Chapter 7.)

[14] J. Ax, *On the units of an algebraic number field*, Illinois J. Math. 9 (1965), 584–589. (Cited in Chapter 6.)

[15] A. Baker, *Rational approximations to* $\sqrt[3]{2}$ *and other algebraic numbers*, Quart. J. Math. Oxford Ser. 15 (1964), 375–383. (Cited in Chapter 4.)

[16] ———, *Linear forms in the logarithms of algebraic numbers. I*, Mathematika 12 (1966), 204–216. (Cited in Chapters 1, 3 & 6.)

[17] ———, *Linear forms in the logarithms of algebraic numbers. II*, Mathematika 14 (1967), 102–107. (Cited in Chapter 1.)

[18] ———, *Linear forms in the logarithms of algebraic numbers. III*, Mathematika 14 (1967), 220–228. (Cited in Chapter 1.)

[19] ———, *Linear forms in the logarithms of algebraic numbers. IV*, Mathematika 15 (1968), 204–216. (Cited in Chapter 1.)

[20] ———, *Contributions to the theory of Diophantine equations.* I*, On the representation of integers by binary forms*, Phil. Trans. R. Soc. London A 263 (1968), 173–191. (Cited in Chapter 4.)

[21] ———, *Contributions to the theory of Diophantine equations.* II*, The Diophantine equation* $y^2 = x^3 + k$, Phil. Trans. R. Soc. London A 263 (1968), 193–208. (Cited in Chapter 4.)

[22] ———, *Bounds for solutions of hyperelliptic equations*, Proc. Cambridge Philos. Soc. 65 (1969), 439–444. (Cited in Chapter 4.)

[23] ———, *On the periods of the Weierstrass* $\wp$*-function*. In: Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), pp. 155–174, Academic Press, London, 1970. (Cited in Chapter 1.)

[24] ———, *Imaginary quadratic fields with class number 2*, Ann. of Math. 94 (1971), 139–152. (Cited in Chapter 3.)

[25] ———, *A sharpening of the bounds for linear forms in logarithms I*, Acta Arith. 21 (1972), 117–129. (Cited in Chapters 1 & 2.)

[26] ———, *A sharpening of the bounds for linear forms in logarithms II*, Acta Arith. 24 (1973), 33–36. (Cited in Chapter 1.)

[27] ———, *A sharpening of the bounds for linear forms in logarithms III*, Acta Arith. 27 (1975), 247–252. (Cited in Chapter 1.)

[28] ———, Transcendental number theory. Cambridge University Press, London-New York, 1975. (Cited in Chapters 1 & 3.)

[29] ———, *Logarithmic forms and the* abc*-conjecture*. In: Number theory (Eger, 1996), 37–44, de Gruyter, Berlin, 1998. (Cited in Chapter 8.)

[30] ———, *Experiments on the* abc*-conjecture*, Publ. Math. Debrecen 65 (2004), 253–260. (Cited in Chapter 8.)

[31] ———, *On an arithmetical function associated with the* abc*-conjecture*. In: Diophantine geometry, 25–33, CRM Series, 4, Ed. Norm., Pisa, 2007. (Cited in Chapter 8.)

[32] A. Baker, B. J. Birch, and E. A. Wirsing, *On a problem of Chowla*, J. Number Theory 5 (1973), 224–236. (Cited in Chapter 3.)

[33] A. Baker and J. Coates, *Integer points on curves of genus* 1, Proc. Cambridge Philos. Soc. 67 (1970), 595–602. (Cited in Chapter 4.)

[34] ———, *Fractional parts of powers of rationals*, Math. Proc. Cambridge Philos. Soc. 77 (1975), 269–279. (Cited in Chapters 1 & 6.)

[35] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford (2) 20 (1969), 129–137. (Cited in Chapter 3.)

[36] A. Baker and C. Stewart, *On effective approximations to cubic irrationals*, New Advances in Transcendence Theory, A. Baker ed., Cambridge University Press, 1988, 1–24. (Cited in Chapter 4.)

[37] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. 442 (1993), 19–62. (Cited in Chapter 2.)

[38] ———, Logarithmic forms and Diophantine geometry. New Mathematical Monographs, 9. Cambridge University Press, Cambridge, 2007. (Cited in Chapters 1, 2 & 3.)

[39] A.S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift for Mat. (5), 4 (1886), 70–80, 130–137. (Cited in Chapter 7.)

[40] G. Barat, R. F. Tichy, and R. Tijdeman, *Digital blocks in linear numeration systems*. In: Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), 607–631, de Gruyter, Berlin, 1999. (Cited in Chapter 3.)

[41] C. F. Barros, On the Lebesgue-Nagell equation and related subjects. PhD Thesis, University of Warwick, 2010. https://homepages.warwick.ac.uk/~maseap/theses/carlosphd.pdf (Cited in Chapter 4.)

[42] M. Bauer and M. A. Bennett, *Applications of the hypergeometric method to the generalized Ramanujan–Nagell equation*, Ramanujan Math. J. 6 (2002), 209–270. (Cited in Chapter 7.)

[43] M. A. Bennett, *Explicit lower bounds for rational approximation to algebraic numbers*, Proc. London Math. Soc. 75 (1997), 63–78. (Cited in Chapter 4.)

[44] ———, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. 498 (1998), 173–199. (Cited in Chapter 3.)

[45] ———, *Rational approximation to algebraic number of small height : The Diophantine equation* $|ax^n - by^n| = 1$, J. Reine Angew. Math. 535 (2001), 1–49. (Cited in Chapter 5.)

[46] ———, Review of 'Catalan's equation with a quadratic exponent' by T. Metsänkylä; MR1816462 (2002a:11021). (Cited in Chapter 4.)

[47] ———, *The Diophantine equation* $(x^k - 1)(y^k - 1) = (z^k - 1)^t$, Indag. Math. (N.S.) 18 (2007), 507–525. (Cited in Chapter 5.)

[48] ———, *Perfect powers with few ternary digits*, Integers 12A, 8pp., 2012. (Cited in Chapter 6.)

[49] ———, *The polynomial-exponential equation* $1 + 2^a + 6^b = y^q$, Period. Math. Hungar. 75 (2017), 387–397. (Cited in Chapter 6.)

[50] M. A. Bennett and N. Billerey, *Sums of two* S*-units via Frey-Hellegouarch curves*, Math. Comp. 86 (2017), 1375–1401. (Cited in Chapter 6.)

[51] M. A. Bennett and Y. Bugeaud, *Effective results for restricted rational approximation to quadratic irrationals*, Acta Arith. 155 (2012), 259–269. (Cited in Chapter 6.)

[52] ———, *Perfect powers with three digits*, Mathematika 60 (2014), 66–84. (Cited in Chapters 2 & 6.)

[53] M. A. Bennett, Y. Bugeaud, and M. Mignotte, *Perfect powers with few binary digits and related Diophantine problems, II*, Math. Proc. Cambridge Philos. Soc. 153 (2012), 525–540. (Cited in Chapter 6.)

[54] ———, *Perfect powers with few binary digits and related Diophantine problems*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) 12 (2013), 941–953. (Cited in Chapters 2 & 6.)

[55] M. A. Bennett and S. R. Dahmen, *Klein forms and the generalized superelliptic equation*, Ann. of Math. 177 (2013), 171–239. (Cited in Chapters 4 & 6.)

[56] M. A. Bennett, M. Filaseta, and O. Trifonov, *Yet another generalization of the Ramanujan-Nagell equation*, Acta Arith. 134 (2008), 211–217. (Cited in Chapter 3.)

[57] ———, *On the factorization of consecutive integers*, J. Reine Angew. Math. 629 (2009), 171–200. (Cited in Chapter 3.)

[58] M. A. Bennett and A. Pintér, *Intersections of recurrence sequences*, Proc. Amer. Math. Soc. 143 (2015), 2347–2353. (Cited in Chapter 9.)

[59] M. A. Bennett and B. M. M. de Weger, *On the Diophantine equation* $|ax^n - by^n| = 1$, Math. Comp. 67 (1998), 413–438. (Cited in Chapter 5.)

[60] A. Bérczes, J.-H. Evertse, and K. Győry, *Effective results for linear equations in two unknowns from a multiplicative division group*, Acta Arith. 136 (2009), 331–349. (Cited in Chapter 4.)

[61] ———, *Effective results for hyper- and superelliptic equations over number fields*, Publ. Math. Debrecen 82 (2013), 727–756. (Cited in Chapters 4 & 6.)

[62] D. J. Bernstein, *Detecting perfect powers in essentially linear time*, Math. Comp. 67 (1998), 1253–1283. (Cited in Chapter 9.)

[63] F. Beukers, The generalised Ramanujan–Nagell Equation, Dissertation, 1979, R. U. Leiden. (Cited in Chapter 7.)

[64] ———, *On the generalized Ramanujan–Nagell equation, I*, Acta Arith. 38 (1980/1981), 389–410. (Cited in Chapter 7.)

[65] ———, *Fractional parts of powers of rationals*, Math. Proc. Cambridge Philos. Soc. 90 (1981), 13–20. (Cited in Chapter 6.)

[66] F. Beukers and C. L. Stewart, *Neighboring powers*, J. Number Theory 130 (2010), 660–679. Addendum: J. Number Theory 130 (2010), 1571. (Cited in Chapter 13.)

[67] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y Zhao, *Bounds on* 2*-torsion in class groups of number fields and integral points on elliptic curves*. Preprint. (Cited in Chapter 13.)

[68] Yu. Bilu, *Effective analysis of integral points on algebraic curves*, Israel J. Math. 90 (1995), 235–252. (Cited in Chapter 4.)

[69] ______, *Quantitative Siegel's theorem for Galois coverings*, Compositio Math. 106 (1997), 125–158. (Cited in Chapter 4.)

[70] ______, *Baker's method and modular curves*. In: A panorama of number theory or the view from Baker's garden (Zürich, 1999), 73–88, Cambridge Univ. Press, Cambridge, 2002. (Cited in Chapter 4.)

[71] ______, Catalan's conjecture (after Mihăilescu). Astérisque No. 294 (2004), vii, 1–26. (Cited in Chapter 4.)

[72] Yu. Bilu et Y. Bugeaud, *Démonstration du théorème de Baker-Feldman via les formes linéaires en deux logarithmes*, J. Théor. Nombres Bordeaux 12 (2000), 13–23. (Cited in Preface and Chapter 4.)

[73] Yu. Bilu, Y. Bugeaud, and M. Mignotte. The Problem of Catalan. Springer, 2014. (Cited in Chapter 4.)

[74] Yu. Bilu and G. Hanrot, *Solving Thue Equations of High Degree*, J. Number Theory 60 (1996), 373–392. (Cited in Chapters 4 & 7.)

[75] ______, *Solving superelliptic Diophantine equations by Baker's method*, Compositio Math. 112 (1998), 273–312. (Cited in Chapter 4.)

[76] ______, *Thue equations with composite fields*, Acta Arith. 88 (1999), 311–326. (Cited in Chapter 4.)

[77] Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*. With an appendix by M. Mignotte. J. Reine Angew. Math. 539 (2001), 75–122. (Cited in Preface and Chapter 7.)

[78] G.D. Birkhoff and H.S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. 5 (1904), 173–180. (Cited in Chapter 7.)

[79] R. Blecksmith, M. Filaseta, and C. Nicol, *A result on the digits of a^n*, Acta Arith. 64 (1993), 331–339. (Cited in Chapter 3.)

[80] A. Blokhuis, A. Brouwer, and B. de Weger, *Binomial collisions and near collisions*. Integers 17 (2017), Paper No. A64, 8 pp. (Cited in Chapter 13.)

[81] R. Bolaño, 2666, Editorial Anagrama, 2004.

[82] E. Bombieri, *On the Thue-Siegel-Dyson Theorem*, Acta Math. 148 (1982) 255–296. (Cited in Chapter 4.)

[83] ______, *Lectures on the Thue principle*. In: Analytic Number Theory and Diophantine Problems (Stillwater, OK, 1984), Progr. Math. 70, Birkhäuser Boston, Boston, MA, 1987, 15–52. (Cited in Chapter 4.)

[84] ______, *Effective Diophantine approximation on $\mathbf{G}_m$*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 20 (1993), 61–89. (Cited in Chapter 4.)

[85] ______, *Forty years of effective results in Diophantine theory*. In: A panorama of number theory or the view from Baker's garden (Zürich, 1999), 194–213, Cambridge Univ. Press, Cambridge, 2002. (Cited in Chapter 4.)

[86] E. Bombieri and P. B. Cohen, *Effective Diophantine Approximation on $\mathbf{G}_m$, II*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 24 (1997), 205–225. (Cited in Chapter 4.)

[87] ———, *An elementary approach to effective Diophantine approximation on* $\mathbf{G}_m$. In: Number Theory and Algebraic Geometry, London Math. Soc. Lecture Note Ser. 303, Cambridge Univ. Press, Cambridge, 2003, 41–62. (Cited in Chapter 4.)

[88] E. Bombieri and W. Gubler, Heights in Diophantine geometry. New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006. (Cited in Chapter 8 and Appendices A & B.)

[89] E. Bombieri and J. Mueller, *On effective measures of irrationality for* $\sqrt[n]{a/b}$ *and related numbers*, J. Reine Angew. Math. 342 (1983), 173–196. (Cited in Chapters 4 & 5 and Appendix A.)

[90] E. Bombieri, A. J. van der Poorten, and J. D. Vaaler, *Effective Measures of Irrationality for Cubic Extensions of Number Fields*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 23 (1996), 211–248. (Cited in Chapter 4 and Appendix A.)

[91] J. Bourgain, E. Lindenstrauss, Ph. Michel, and A. Venkatesh, *Some effective results for* $\times a \times b$, Ergodic Theory Dynam. Systems 29 (2009), 1705–1722. (Cited in Chapter 3.)

[92] B. Brindza, *On* S*-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hungar. 44 (1984), 133–139. (Cited in Chapter 4.)

[93] ———, *On* S*-integral solutions of the Catalan equation*, Acta Arith. 48 (1987), 397–412. (Cited in Chapter 6.)

[94] ———, *Thue equations and multiplicative independence*. In: Number Theory and Cryptography (Sydney 1989), London Math. Soc. Lecture Note Ser., 154, Cambridge Univ. Press, Cambridge, 1990, 213–220. (Cited in Chapter 9.)

[95] B. Brindza, J. H. Evertse, and K. Győry, *Bounds for the solutions of some diophantine equations in terms of discriminants*, J. Austral. Math. Soc. (Series A) 51 (1991), 8–26. (Cited in Chapter 4 and Appendix C.)

[96] B. Brindza and K. Győry, *On unit equations with rational coefficients*, Acta Arith. 53 (1990), 367–388. (Cited in Chapter 9.)

[97] B. Brindza, K. Győry, and R. Tijdeman, *On the Catalan equation over algebraic number fields*, J. Reine Angew. Math. 367 (1986), 90–102. (Cited in Chapter 4.)

[98] J. Browkin, *The* abc*-conjecture for algebraic numbers*, Acta Math. Sin. (Engl. Ser.) 22 (2006), 211–222. (Cited in Chapter 8.)

[99] A. Brumer, *On the units of algebraic number fields*, Mathematika 14 (1967), 121–124. (Cited in Chapters 1 & 6.)

[100] Y. Bugeaud, *Sur la distance entre deux puissances pures*, C. R. Acad. Sci. Paris 322 (1996), 1119–1121. (Cited in Chapter 4.)

[101] ———, *Bounds for the solutions of superelliptic equations*, Compositio Math. 107 (1997), 187–219. (Cited in Chapters 4 & 6.)

[102] ———, *On the Diophantine equation* $x^2 - 2^m = \pm y^n$, Proc. Amer. Math. Soc. 125 (1997), 3203–3208. (Cited in Chapter 6.)

[103] ———, *On the diophantine equation* $x^2 - p^m = \pm y^n$, Acta Arith. 80 (1997), 213–223. (Cited in Chapter 6.)

[104] ______, *On the greatest prime factor of* $(ab+1)(bc+1)(ca+1)$, Acta Arith. 86 (1998), 45–49. (Cited in Chapter 9.)

[105] ______, *Algebraic numbers close to* 1 *in non-Archimedean metrics*, Ramanujan J. 2 (1998), 449–457. (Cited in Chapter 2.)

[106] ______, *Sur le plus grand facteur premier de* $ax^n + by^m$, C. R. Acad. Sci. Paris 326 (1998), 661–665. (Cited in Chapter 6.)

[107] ______, *Bornes effectives pour les solutions des équations en* S*-unités et des équations de Thue-Mahler*, J. Number Theory 71 (1998), 227–244. (Cited in Chapter 4.)

[108] ______, *On the greatest prime factor of* $\alpha x^n + \beta y^m$, Proceedings of the Number Theory Conference, Eger 1996, Eds. Győry, Pethő, Sós. De Gruyter (1998), 115–122. (Cited in Chapter 6.)

[109] ______, *Linear forms in* p*-adic logarithms and the Diophantine equation* $\frac{x^n-1}{x-1} = y^q$, Math. Proc. Cambridge Philos. Soc. 127 (1999), 373–381. (Cited in Chapters 2, 6 & 12.)

[110] ______, *On the greatest prime factor of* $ax^m + by^n$*, II*, Bull. London Math. Soc. 32 (2000), 673–678. (Cited in Chapter 6.)

[111] ______, *Linear forms in two* m*-adic logarithms and applications to Diophantine problems*, Compositio Math. 132 (2002), 137–158. (Cited in Chapters 2 & 6.)

[112] ______, *On the Diophantine equation* $(x^k-1)(y^k-1) = (z^k-1)$, Indag. Math. (N.S.) 15 (2004), 21–28. (Cited in Chapter 5.)

[113] ______, Approximation by algebraic numbers. Cambridge Tracts in Mathematics 160, Cambridge, 2004. (Cited in Chapters 4 & 10 and Appendix A.)

[114] ______, *Linear forms in the logarithms of algebraic numbers close to 1 and applications to Diophantine equations*, Proceedings of the Number Theory conference DION 2005, Mumbai, pp. 59–76, Narosa Publ. House, 2008. (Cited in Chapter 5.)

[115] ______, *On the convergents to algebraic numbers*. In: Analytic number theory, 133–143, Cambridge Univ. Press, Cambridge, 2009. (Cited in Chapters 3 & 13.)

[116] ______, *Effective irrationality measures for quotients of logarithms of rational numbers*, Hardy-Ramanujan J. 38 (2015), 45–48. (Cited in Chapter 5.)

[117] ______, *Effective irrationality measures for real and p-adic roots of rational numbers close to* 1*, with an application to parametric families of Thue–Mahler equations*, Math. Proc. Cambridge Phil. Soc. 164 (2018), 99–108. (Cited in Chapters 2, 5 & 6.)

[118] ______, *On the digital representation of integers with bounded prime factors*, Osaka Math. J. To appear. (Cited in Chapter 6.)

[119] Y. Bugeaud, M. Cipu, and M. Mignotte, *On the representation of Fibonacci and Lucas numbers in an integer base*, Ann. Math. Qué. 37 (2013), 31–43. (Cited in Chapter 3.)

[120] Y. Bugeaud and A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. 135 (2003), 1–10. (Cited in Chapter 5.)

[121] Y. Bugeaud and J.-H. Evertse, *On S-parts of linear recurrence sequences*, Mathematika 63 (2017), 840–851. (Cited in Chapter 3.)

[122] Y. Bugeaud, J.-H. Evertse, and K. Győry, *S-parts of values of univariate polynomials, binary forms and decomposable forms at integral points*. Preprint. (Cited in Chapters 3 & 6.)

[123] Y. Bugeaud and K. Gyarmati, *On generalizations of a problem of Diophantus*, Illinois J. Math. 48 (2004), 1105–1115. (Cited in Chapter 5.)

[124] Y. Bugeaud and K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. 74 (1996), 67–80. (Cited in Chapters 4 & 6 and Appendix C.)

[125] ______, *Bounds for the solutions of Thue–Mahler equations and norm form equations*, Acta Arith. 74 (1996), 273–292. (Cited in Chapters 4 & 6.)

[126] ______, *On binomial Thue–Mahler equations*, Period. Math. Hungar. 49 (2004), 25–34. (Cited in Chapters 6 & 7.)

[127] Y. Bugeaud, G. Hanrot et M. Mignotte, *Sur l'équation diophantienne $\frac{x^n-1}{x-1} = y^q$, III*, Proc. London Math. Soc. 84 (2002), 59–78. (Cited in Chapter 4.)

[128] Y. Bugeaud and H. Kaneko, *On the digital representation of smooth numbers*, Math. Proc. Cambridge Philos. Soc. To appear. (Cited in Chapter 6.)

[129] Y. Bugeaud et M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory 61 (1996), 311–342. (Cited in Chapters 2, 6 & 12.)

[130] Y. Bugeaud and F. Luca, *A quantitative lower bound for the greatest prime factor of $(ab+1)(bc+1)(ca+1)$*, Acta Arith. 114 (2004), 275–294. (Cited in Chapter 9.)

[131] Y. Bugeaud, F. Luca, M. Mignotte, and S. Siksek, *On perfect powers in Lucas sequences*, Int. J. Number Theory 1 (2005), 309–332. (Cited in Chapter 7.)

[132] Y. Bugeaud and M. Mignotte, *On integers with identical digits*, Mathematika 46 (1999), 411–417. (Cited in Chapter 6.)

[133] ______, *L'équation de Nagell-Ljunggren $\frac{x^n-1}{x-1} = y^q$*, Enseign. Math. (2) 48 (2002), 147–168. (Cited in Chapters 6 & 13.)

[134] Y. Bugeaud, M. Mignotte et F. Normandin, *Nombres algébriques de petite mesure et formes linéaires en un logarithme*, C. R. Acad. Sci. Paris Sér. I Math. 321 (1995), 517–522. (Cited in Chapter 2.)

[135] Y. Bugeaud, M. Mignotte, and Y. Roy, *On the Diophantine equation $\frac{x^n-1}{x-1} = y^q$*, Pacific J. Math. 193 (2000), 257–268. (Cited in Chapter 6.)

[136] Y. Bugeaud, M. Mignotte, Y. Roy, and T. N. Shorey, *The diophantine equation $(x^n-1)/(x-1) = y^q$ has no solution with x square*, Math. Proc. Cambridge Philos. Soc. 127 (1999), 353–372. (Cited in Chapter 5.)

[137] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. of Math. 163 (2006), 969–1018. (Cited in Chapters 3 & 7.)

[138] ———, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell Equation*, Compos. Math. 142 (2006), 31–62. (Cited in Chapters 4 & 7.)

[139] Y. Bugeaud and T. N. Shorey, *On the number of solutions of the generalized Ramanujan–Nagell equation*, J. Reine Angew. Math. 539 (2001), 55–74. (Cited in Chapter 7.)

[140] ———, *On the Diophantine equation* $(x^m - 1)/(x - 1) = (y^n - 1)/(y - 1)$, Pacific J. Math. 207 (2002), 61–75. (Cited in Chapter 5.)

[141] E. Burger and R. Tubbs, Making transcendence transparent. An intuitive approach to classical transcendental number theory. Springer-Verlag, New York, 2004. (Cited in Chapter 1.)

[142] P. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. 15 (1913), 30–70. (Cited in Chapter 7.)

[143] M. Carrizosa, *Survey on Lehmer problems*, São Paulo J. Math. Sci. 3 (2009), 317–327. (Cited in Chapter 10.)

[144] J. W. S. Cassels, An introduction to Diophantine Approximation. Cambridge Tracts in Math. and Math. Phys., vol. 99, Cambridge University Press, 1957. (Cited in Chapter 3 and Appendix A.)

[145] E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, J. Reine Angew. Math. 27 (1844), 192. (Cited in Chapter 4.)

[146] C. K. Chi, New explicit result related to the abc-conjecture. MPhil. thesis, Hong Kong Univ. of Science and Technology, 2005. (Cited in Chapter 8.)

[147] K. C. Chim and V. Ziegler, *On Diophantine equations involving sums of Fibonacci numbers and powers of* 2. Preprint. (Cited in Chapter 3.)

[148] G. V. Chudnovsky, *On the method of Thue-Siegel*, Ann. of Math. 117 (1983), 325–382. (Cited in Chapter 4.)

[149] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), 279–305. (Cited in Chapter 1.)

[150] ———, *An effective p-adic analogue of a theorem of Thue, II*, Acta Arith. 16 (1970), 399–412. (Cited in Chapter 6.)

[151] J. Coates and S. Lang, *Diophantine approximation on Abelian varieties with complex multiplication*, Invent. Math. 34 (1976), 129–133. (Cited in Chapter 1.)

[152] H. Cohen, Démonstration de la conjecture de Catalan. In: Théorie algorithmique des nombres et équations diophantiennes, 1–83, Ed. Éc. Polytech., Palaiseau, 2005. (Cited in Chapter 4.)

[153] ———, Number Theory. Vol. I. Tools and Diophantine equations. Graduate Texts in Math. 239, Springer, 2007. (Cited in Chapter 4.)

[154] ———, Number Theory. Vol. II. Analytic and Modern Tools. Graduate Texts in Math. 240, Springer, 2007. (Cited in Chapter 4.)

[155] J. H. E. Cohn, *The Diophantine equation $x^2 + C = y^n$*, Acta Arith. 65 (1993), 367–381. (Cited in Chapters 4 & 7.)

[156] P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. 149 (2002), 431–451. (Cited in Chapter 3.)

[157] ______, *On the greatest prime factor of $(ab + 1)(ac + 1)$*, Proc. Amer. Math. Soc. 131 (2003), 1705–1709. (Cited in Chapter 9.)

[158] ______, *On the rational approximations to the powers of an algebraic number: solution of two problems of Mahler and Mendès France*, Acta Math. 193 (2004), 175–191. (Cited in Chapter 6.)

[159] ______, *Finiteness of odd perfect powers with four nonzero binary digits*, Ann. Inst. Fourier (Grenoble) 63 (2013), 715–731. (Cited in Chapter 6.)

[160] L. V. Danilov, *The Diophantine equation $x^3 - y^2 = k$ and Hall's conjecture*, Math. Notes Acad. Sci. USSR 32 (1982), 617–618. (Cited in Chapter 13.)

[161] ______, *The Diophantine equations $x^m - Ay^n = k$*, Mat. Zametki 46 (1989), 38–45, 126 (in Russian); English translation in Math. Notes 46 (1989), 914–919. (Cited in Chapter 13.)

[162] S. David, *Minorations de formes linéaires de logarithmes elliptiques*. Mém. Soc. Math. France (N.S.) No. 62 (1995). (Cited in Chapter 1.)

[163] S. David and N. Hirata-Kohno, *Linear forms in elliptic logarithms*, J. Reine Angew. Math. 628 (2009), 37–89. (Cited in Chapter 1.)

[164] H. Derksen and D. Masser, *Linear equations over multiplicative groups, recurrences, and mixing II*, Indag. Math. (N.S.) 26 (2015), 113–136. (Cited in Chapter 13.)

[165] G. A. Dill, *Effective approximation and Diophantine applications*, Acta Arith. 177 (2017), 169–199. (Cited in Chapter 4.)

[166] L. G. P. Dirichlet, *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einige Anwendungen auf die Theorie der Zahlen*, S.-B. Preuss. Akad. Wiss. (1842), 93–95. (Cited in Appendix A.)

[167] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401. (Cited in Chapter 10.)

[168] P. Dong, *Minoration de combinaisons linéaires de deux logarithmes p-adiques*, Ann. Fac. Sci. Toulouse Math. (5) 12 (1991), 195–250. (Cited in Chapters 1 & 2.)

[169] ______, *Minorations de combinaisons linéaires de logarithmes p-adiques de nombres algébriques*, Dissertationes Math. (Rozprawy Mat.) 343 (1995), 97 pp. (Cited in Chapters 1, 2 & 9.)

[170] K. A. Draziotis, *On the number of integer points on the elliptic curve $y^2 = x^3 + Ax$*, Int. J. Number Theory 7 (2011), 611–621. (Cited in Chapter 13.)

[171] A. Dubickas, *On algebraic numbers close to* 1, Bull. Austral. Math. Soc. 58 (1998), 423–434. (Cited in Chapter 2.)

[172] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183–214. (Cited in Chapter 3.)

[173] ———, *On Hall's conjecture*, Acta Arith. 147 (2011), 397–402. (Cited in Chapter 13.)

[174] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441. (Cited in Chapter 7.)

[175] ———, *Exceptional real Lucas sequences*, Pacific J. Math. 11 (1961), 489–494. (Cited in Chapter 7.)

[176] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*, Algorithmic number theory (Leiden, 2000), 33–63, Lecture Notes in Comput. Sci. 1838, Springer, Berlin, 2000. (Cited in Chapter 13.)

[177] P. Erdős, *Some recent advances and current problems in number theory*. In: Lectures on Modern Mathematics, Vol. III, pp. 196–244, Wiley, New York, 1965. (Cited in Chapter 7.)

[178] G. Everest and K. Győry, *On some arithmetical properties of solutions of decomposable form equations*, Math. Proc. Cambridge Philos. Soc. 139 (2005), 27–40. (Cited in Chapter 6.)

[179] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, Recurrence sequences. Mathematical Surveys and Monographs, 104. American Mathematical Society, Providence, RI, 2003. (Cited in Chapter 3.)

[180] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. 53 (1984), 225–244. (Cited in Chapters 3 & 13.)

[181] J.-H. Evertse and R. G. Ferretti, *A further improvement of the quantitative subspace theorem*, Ann. of Math. 177 (2013), 513–590. (Cited in Chapter 13.)

[182] J. H. Evertse and K. Győry, Unit equations in Diophantine number theory. Cambridge Studies in Advanced Mathematics 146, Cambridge University Press, 2015. (Cited in Preface, Chapters 4 & 6, and Appendix C.)

[183] ———, Discriminant equations in Diophantine number theory. New Mathematical Monographs 32, Cambridge University Press, 2016. (Cited in Chapters 2, 4 & 6 and Appendix B.)

[184] J. H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman, *S-unit equations and their applications*. In: New Advances in Transcendence Theory (Ed. A. Baker), 110–174. Cambridge University Press, 1988. (Cited in Chapter 6.)

[185] N. I. Feldman, *Improved estimate for a linear form of the logarithms of algebraic numbers*, Mat. Sb. 77 (1968), 256–270 (in Russian). English translation in Math. USSR. Sb. 6 (1968) 393–406. (Cited in Chapters 1, 4 & 11.)

[186] ———, *Une amélioration effective de l'exposant dans le théorème de Liouville*, Izv. Akad. Nauk 35 (1971), 973–990 (in Russian). English translation in Math. USSR Izv. 5 (1971), 985–1002. (Cited in Chapter 1.)

[187] M. van Frankenhuysen, *A lower bound in the abc conjecture*, J. Number Theory 82 (2000), 91–95. (Cited in Chapter 8.)

[188] C. Fuchs, R. von Känel, and G. Wüstholz, *An effective Shafarevich theorem for elliptic curves*, Acta Arith. 148 (2011), 189–203. (Cited in Chapter 4.)

[189] C. Fuchs and D. H. Pham, *Commutative algebraic groups and p-adic linear forms*, Acta Arith. 169 (2015), 115–147. (Cited in Chapter 1.)

[190] C. Fuchs and R. F. Tichy, *Perfect powers in linear recurring sequences*, Acta Arith. 107 (2003), 9–25. (Cited in Chapter 3.)

[191] I. Gaál, Diophantine equations and power integral bases. New computational methods. Birkhäuser Boston, Inc., Boston, MA, 2002. (Cited in Chapter 4.)

[192] É. Gaudron, *Mesures d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif*, Invent. Math. 162 (2005), 137–188. (Cited in Chapter 1.)

[193] ______, *Formes linéaires de logarithmes effectives sur les variétés abéliennes*, Ann. Sci. École Norm. Sup. 39 (2006), 699–773. (Cited in Chapter 1.)

[194] ______, *Étude du cas rationnel de la théorie des formes linéaires de logarithmes*, J. Number Theory 127 (2007), 220–261. (Cited in Chapter 1.)

[195] ______, *Minorations simultanées de formes linéaires de logarithmes de nombres algébriques*, Bull. Soc. Math. France 142 (2014), 1–62. (Cited in Chapter 9.)

[196] J. Gebel, A. Pethő, and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. 68 (1994), 171–192. (Cited in Chapter 1.)

[197] A. O. Gelfond, *On Hilbert's seventh problem*, Dokl. Akad. Nauk SSSR 2 (1934), 1–3 (in Russian) and 4–6 (in French) *Sur le septième problème de Hilbert*, Izv. Akad. Nauk SSSR 7 (1934), 623–630. (Cited in Chapter 1.)

[198] ______, *Sur les approximations des nombres transcendants par des nombres algébriques*, C. R. Acad. Sc. URSS 2 (1935), 177–182. (Cited in Chapter 1.)

[199] ______, *Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier*, Mat. Sb. 7 (1940), 7–25. (Cited in Chapters 1 & 6.)

[200] ______, Transcendental and algebraic numbers. Dover publ., New York, 1960. (Cited in Chapters 1 & 6.)

[201] A. Gorodnik and R. Spatzier, *Mixing properties of commuting nilmanifold automorphisms*, Acta Math. 215 (2015), 127–159. (Cited in Chapter 3.)

[202] N. Gouillon, *Explicit lower bounds for linear forms in two logarithms*, J. Théor. Nombres Bordeaux 18 (2006), 125–146. (Cited in Chapters 2 & 5.)

[203] F. Q. Gouvêa, p-adic numbers. Universitext. Springer-Verlag, Berlin, 1993. (Cited in Appendix F.)

[204] C. A. Grimm, *A conjecture on consecutive composite numbers*, Amer. Math. Monthly 76 (1969), 1126–1128. (Cited in Chapter 13.)

[205] S. S. Gross and A. F. Vincent, *On the factorization of $f(n)$ for $f(x)$ in $\mathbb{Z}[x]$*, Int. J. Number Theory 9 (2013), 1225–1236. (Cited in Chapter 3.)

[206] R. K. Guy, Unsolved problems in number theory. Springer-Verlag, New York, 1994 (Cited in Chapter 6.)

[207] K. Gyarmati, A. Sárközy, and C.L. Stewart, *On shifted products which are powers*, Mathematika 49 (2002), 227–230. (Cited in Chapter 5.)

[208] K. Gyarmati and C. L. Stewart, *On powers in shifted products*, Glas. Mat. 42 (2007), 273–279. (Cited in Chapter 5.)

[209] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. 23 (1973), 419–426. (Cited in Chapter 4.)

[210] ———, *Sur les polynômes à coefficients entiers et de discriminant donné. II*, Publ. Math. Debrecen 21 (1974), 125–144. (Cited in Chapter 4.)

[211] ———, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. 54 (1979), 583–600. (Cited in Chapter 6.)

[212] ———, *Explicit upper bounds for the solutions of some Diophantine equations*, Ann. Acad. Sci. Fenn. Ser. A I Math. 5 (1980), 3–12. (Cited in Chapter 6.)

[213] ———, *On some arithmetical properties of Lucas and Lehmer numbers. II*, Acta Acad. Paedagog. Agriensis Sect. Mat. 30 (2003), 67–73. (Cited in Chapter 7.)

[214] ———, *On the abc conjecture in algebraic number fields*, Acta Arith. 133 (2008), 281–295. (Cited in Chapter 8.)

[215] K. Győry, M. Mignotte, and T. N. Shorey, *On some arithmetical properties of weighted sums of S-units*, Math. Pannon. 1 (1990), 25–43. (Cited in Chapter 6.)

[216] K. Győry and Z. Z. Papp, *Effective estimates for the integer solutions of norm form and discriminant form equations*, Publ. Math. Debrecen 25 (1978), 311–325. (Cited in Chapter 4.)

[217] K. Győry and K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. 123 (2006), 9–41. (Cited in Chapters 3, 4, 6 & 8.)

[218] H. Halberstam and H.-E. Richert, Sieve methods. London Mathematical Society Monographs, No. 4. Academic Press, London-New York, 1974. (Cited in Appendix D.)

[219] M. Hall Jr., *The Diophantine equation $x^3 - y^2 = k$*. In: A. Atkin, B. Birch (Eds.), Computers in Number Theory, Academic Press, 1971, pp. 173–198. (Cited in Chapter 13.)

[220] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 5th. edition, Clarendon Press, 1979. (Cited in Chapter 6 and Appendices A & D.)

[221] J. Haristoy, Équations diophantiennes exponentielles. Thèse, University of Strasbourg I (Louis Pasteur), Strasbourg, 2003. Prépublication de l'Institut de Recherche Mathématique Avancée, 2003/29, Strasbourg, 2003. 76 pp. (Cited in Chapters 3 & 6.)

[222] S. Harrap and A. Haynes, *The mixed Littlewood conjecture for pseudo-absolute values*, Math. Ann. 357 (2013), 941–960. (Cited in Chapter 3.)

[223] H. Hasse, Number theory. Grundlehren der Mathematischen Wissenschaften, 229. Springer-Verlag, Berlin-New York, 1980. (Cited in Appendix F.)

[224] M. Hata, *A lower estimate for* $\|e^n\|$, J. Number Theory 130 (2010), 1685–1704. (Cited in Chapter 13.)

[225] H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and* 3*-torsion in class groups*, J. Amer. Math. Soc. 19 (2006), 527–550. (Cited in Chapter 13.)

[226] S. Hernández and F. Luca, *On the largest prime factor of* $(ab+1)(ac+1)(bc+1)$, Bol. Soc. Mat. Mexicana 9 (2003), 235–244. (Cited in Chapter 9.)

[227] C. Heuberger, *Parametrized Thue equations – A survey*. In: Proceedings of the RIMS symposium 'Analytic Number Theory and Surrounding Areas', Kyoto, Oct. 18–22, 2004, RIMS Kôkyûroku, vol. 1511, 2006, pp. 82–91. (Cited in Chapter 4.)

[228] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl* n^{ter} *Potenzen* (*Waringsches Problem*), Math. Ann. 67 (1909), 281–300. (Cited in Chapter 6.)

[229] N. Hirata-Kohno, *Formes linéaires de logarithmes de points algébriques sur les groupes algébriques*, Invent. Math. 104 (1991), 401–433. (Cited in Chapter 1.)

[230] ———, *Approximations simultanées sur les groupes algébriques commutatifs*, Compositio Math. 86 (1993), 69–96. (Cited in Chapter 1.)

[231] N. Hirata-Kohno and T. N. Shorey, *On the equation* $(x^m-1)/(x-1) = y^q$ *with* x *power*. In: Analytic Number Theory (Kyoto, 1996), 119–125, London Math. Soc. Lecture Note Ser. 247, Cambridge Univ. Press, Cambridge, 1997. (Cited in Chapter 5.)

[232] N. Hirata-Kohno and R. Takada, *Linear forms in two elliptic logarithms in the* p*-adic case*, Kyushu J. Math. 64 (2010), 239–260. (Cited in Chapter 1.)

[233] A. Hoshi, *Complete solutions to a family of Thue equations of degree* 12, J. Théor. Nombres Bordeaux 29 (2017), 549–568. (Cited in Chapter 4.)

[234] R. Juricevic, *Explicit estimates of solutions of some Diophantine equations*, Funct. Approx. Comment. Math. 38 (2008), 171–194. (Cited in Chapter 13.)

[235] R. von Känel, *An effective proof of the hyperelliptic Shafarevich conjecture*, J. Théor. Nombres Bordeaux 26 (2014), 507–530. (Cited in Chapter 4.)

[236] ———, *Integral points on moduli schemes of elliptic curves*, Trans. London Math. Soc. 1 (2014), 85–115. (Cited in Chapter 8.)

[237] R. von Känel and B. Matschke, *Solving* S*-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture*. Preprint. (Cited in Chapters 6 & 8.)

[238] R. M. Kaufman, *An estimate of a linear form of logarithms of algebraic numbers in a* p*-adic metric*, Vestnik Moskov. Univ. Ser. I Mat. Meh. 26 (1971), 3–10 (in Russian). (Cited in Chapter 1.)

[239] A. Ya. Khintchine, Continued Fractions. The University of Chicago Press, Chicago Ill., London, 1964. (Cited in Appendix A.)

[240] D. Kim, *A modular approach to cubic Thue–Mahler equations*, Math. Comp. 86 (2017), 1435–1471. (Cited in Chapter 6.)

[241] J. Kim and C. L. Stewart, *Well spaced integers generated by an infinite set of primes*, Proc. Amer. Math. Soc. 143 (2015), 915–923. (Cited in Chapter 3.)

[242] N. Koblitz, p-adic numbers, p-adic analysis, and zeta-functions. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984. (Cited in Appendix F.)

[243] J. F. Koksma, Diophantische Approximationen, Ergebnisse d. Math. u. ihrer Grenzgebiete, vol. 4, Springer, 1936. (Cited in Chapter 1.)

[244] P. H. Koymans, *The Catalan equation*, Indag. Math. (N. S.) 28 (2017), 321–352. (Cited in Chapter 6.)

[245] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), 173–175. (Cited in Appendix B.)

[246] J. F. Kubina and M. C. Wunderlich, *Extending Waring's conjecture to* 471, 600, 000, Math. Comp. 55 (1990), 815–820. (Cited in Chapter 6.)

[247] L. Kühne, *An effective result of André–Oort type*, Ann. of Math. 176 (2012), 651–671. (Cited in Chapter 3.)

[248] ______, *Logarithms of algebraic numbers*, J. Théor. Nombres Bordeaux 27 (2015), 499–535. (Cited in Chapter 13.)

[249] A. Kulkarni, N. M. Mavraki, and K. D. Nguyen, *Algebraic approximations to linear combinations of powers: an extension of results by Mahler and Corvaja–Zannier*. Trans. Amer. Math. Soc. To appear. (Cited in Chapters 6 & 13.)

[250] S. Lang, Elliptic curves: Diophantine analysis, Grundlehren der Mathematischen Wissenschaften 231, Springer–Verlag, Berlin–New York, 1978. (Cited in Chapters 8 & 13.)

[251] M. Langevin, *Quelques applications de nouveaux résultats de Van der Poorten*. In: Séminaire Delange-Pisot-Poitou, 17e année (1975/76), Théorie des nombres: Fasc. 2, Exp. No. G12, 11 pp. Secrétariat Math., Paris (1977). (Cited in Chapter 4.)

[252] M. Laurent, *Linear forms in two logarithms and interpolation determinants*, Acta Arith. 66 (1994), 181–199. (Cited in Chapters 2 & 11.)

[253] ______, *Linear forms in two logarithms and interpolation determinants. II*, Acta Arith. 133 (2008), 325–348. (Cited in Chapters 2 & 11.)

[254] M. Laurent, M. Mignotte et Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321. (Cited in Chapters 2, 3, 4 & 11.)

[255] M. Le, *A note on the diophantine equation* $(x^m - 1)/(x - 1) = y^n$, Acta Arith. 64 (1993), 19–28. (Cited in Chapter 6.)

[256] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. 9 (1850), 178–181. (Cited in Chapter 4.)

[257] A.-M. Legendre, Théorie des nombres, troisième édition, Tome 1, Paris, 1830. (Cited in Appendix A.)

[258] H. W. Lenstra and J. O. Shallit, *Continued fractions and linear recurrences*, Math. Comp. 61 (1993), 351–354. (Cited in Chapter 7.)

[259] M.-G. Leu and G.-W. Li, *The Diophantine equation* $2x^2 + 1 = 3^n$, Proc. Amer. Math. Soc. 131 (2003), 3643–3645. (Cited in Chapter 7.)

[260] W. J. LeVeque, Fundamentals of number theory. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977. (Cited in Appendix C.)

[261] C. Levesque and M. Waldschmidt, *Some remarks on diophantine equations and diophantine approximation*, Vietnam J. Math. 39 (2011), 343–368. (Cited in Chapter 4.)

[262] ______, *Familles d'équations de Thue–Mahler n'ayant que des solutions triviales*, Acta Arith. 155 (2012), 117–138. (Cited in Chapter 6.)

[263] A. Levin, *Linear forms in logarithms and integral points on higher-dimensional varieties*, Algebra Number Theory 8 (2014), 647–687. (Cited in Chapter 6.)

[264] J. Liouville, *Remarques relatives à des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques*, C. R. Acad. Sci. Paris 18 (1844), 883–885 et 910–911. (Cited in Chapter 1 and Appendix A.)

[265] W. Ljunggren, *Über die unbestimmte Gleichung* $Ax^2 - By^4 = C$, Arch. f. Mat. og Naturvid. 41 (1938), No. 10, 18 pp. (Cited in Chapter 3.)

[266] ______, *On the diophantine equation* $x^2 + 4 = Ay^2$, Det. Kgl. Norske Vid.-Selsk. Forh. 24 (1951), No. 18, 82–84. (Cited in Chapter 3.)

[267] T. Loher and D. Masser, *Uniformly counting points of bounded height*, Acta Arith. 111 (2004), 277–297. (Cited in Chapter 10.)

[268] H. London and R. Finkelstein, *On Fibonacci and Lucas numbers which are perfect powers*, Fibonacci Quart. 5 (1969), 476–481. (Cited in Chapter 3.)

[269] R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*, C. R. Acad. Sci. Paris Sér. I Math. 296 (1983), 707–708. (Cited in Chapter 10.)

[270] J. H. Loxton, *Some problems involving powers of integers*, Acta Arith. 46 (1986), 113–123. (Cited in Chapter 9.)

[271] J. H. Loxton and A. J. van der Poorten, *Multiplicative dependence in number fields*, Acta Arith. 42 (1983), 291–302. (Cited in Chapters 2 & 10.)

[272] F. Luca, *Distinct digits in base b expansions of linear recurrence sequences*, Quaest. Math. 23 (2000), 389–404. (Cited in Chapter 3.)

[273] ______, *On a conjecture of Erdős and Stewart*, Math. Comp. 70 (2001), 893–896. (Cited in Chapter 6.)

[274] ______, *The Diophantine equation* $x^2 = p^a \pm p^b + 1$, Acta Arith. 112 (2004), 87–101. (Cited in Chapter 6.)

[275] ______, *On shifted products which are powers*, Glas. Mat. 40 (2005), 13–20. (Cited in Chapter 5.)

[276] ______, *Repdigits as sums of three Fibonacci numbers*, Math. Commun. 17 (2012), 1–11. (Cited in Chapter 3.)

[277] F. Luca and M. Mignotte, *Arithmetic properties of the integer part of the powers of an algebraic number*, Glas. Mat. Ser. III 44 (2009), 285–307. (Cited in Chapter 3.)

[278] K. Mahler, *Ein Beweis der Transzendenz der P-adischen Exponentialfunktion*, J. Reine Angew. Math. 169 (1932), 61–66. (Cited in Chapter 1.)

[279] ______, *Zur Approximation algebraischer Zahlen. I*, Math. Ann. 107 (1933), 691–730. (Cited in Chapter 6.)

[280] ______, *Über transzendente P-adische Zahlen*, Compositio Math. 2 (1935), 259–275. (Cited in Chapter 1.)

[281] ______, *On the approximation of logarithms of algebraic numbers*, Philos. Trans. R. Soc. Lond. Ser. A 245 (1953), 371–398. (Cited in Chapter 13.)

[282] ______, *On the fractional parts of the powers of a rational number, II*, Mathematika 4 (1957), 122–124. (Cited in Chapter 6.)

[283] G. Martin and W. Miao, *abc triples*, Funct. Approx. Comment. Math. 55 (2016), 145–176. (Cited in Chapter 8.)

[284] D. W. Masser, Elliptic functions and transcendence. Lecture Notes in Mathematics, Vol. 437. Springer-Verlag, Berlin-New York, 1975. (Cited in Chapter 1.)

[285] ______, Open problems. Proc. Symp. Analytic Number Th. W. W. L. Chen (ed.). London: Imperial College 1985. (Cited in Chapter 8.)

[286] ______, *On abc and discriminants*, Proc. Amer. Math. Soc. 130 (2002), 3141–3150. (Cited in Chapter 8.)

[287] ______, Auxiliary polynomials in number theory. Cambridge Tracts in Mathematics, 207. Cambridge University Press, Cambridge, 2016. (Cited in Chapter 10.)

[288] ______, *Abcological anecdotes*, Mathematika 63 (2017), 713–714. (Cited in Chapter 8.)

[289] E. M. Matveev, *Linear and multiplicative relations*, Mat. Sb. 184 (1993), 23–40 (in Russian); English translation in Russian Acad. Sci. Sb. Math. 78 (1994), 411–425. (Cited in Chapter 10.)

[290] ______, *Explicit lower estimates for rational homogeneous forms in logarithms of algebraic numbers*, Izv. Akad. Nauk SSSR Ser. Mat. 62 (1998), 81–136 (in Russian); English translation in Izv. Math. 62 (1998), 723–772. (Cited in Chapter 2.)

[291] ______, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Acad. Nauk Ser. Mat. 64 (2000), 125–180 (in Russian); English translation in Izv. Math. 64 (2000), 1217–1269. (Cited in Chapter 2.)

[292] ______, *On the index of multiplicative groups of algebraic numbers*, Mat. Sb. 196 (2005), 59–70 (in Russian); English translation in Sb. Math. 196 (2005), 1307–1318. (Cited in Chapter 10.)

[293] M. Mignotte, *A note on linear recursive sequences*, J. Austral. Math. Soc. 20 (1975), 242–244. (Cited in Chapter 13.)

[294] ———, *Intersection des images de certaines suites récurrentes linéaires*, Theoret. Comput. Sci. 7 (1978), 117–122. (Cited in Chapter 3.)

[295] ———, *Sur les entiers qui s'écrivent simplement en différentes bases*, European J. Combin. 9 (1988), 307–316. (Cited in Chapter 3.)

[296] ———, *A note on the equation $ax^n - by^n = c$*, Acta Arith. 75 (1996), 287–295. (Cited in Chapter 5.)

[297] ———, *Catalan's equation just before 2000*. In: Number theory (Turku, 1999), 247–254, de Gruyter, Berlin, 2001. (Cited in Chapter 4.)

[298] ———, *A kit on linear forms in three logarithms*, http://www-irma.u-strasbg.fr/~bugeaud/travaux/kit.pdf (Cited in Chapters 2 & 3.)

[299] M. Mignotte, T. N. Shorey, and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math. 349 (1984), 63–76. (Cited in Chapter 13.)

[300] M. Mignotte and M. Waldschmidt, *On algebraic numbers of small height: linear forms in one logarithm*, J. Number Theory 47 (1994), 43–62. (Cited in Chapter 2.)

[301] M. Mignotte and B. M. M. de Weger, *On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$*, Glasgow Math. J. 38 (1996), 77–85. (Cited in Chapter 4.)

[302] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. 572 (2004), 167–195. (Cited in Chapter 4.)

[303] De Ze Mo, *Exponential Diophantine equations with four terms. II*, Acta Math. Sinica 37 (1994), 482–490. (Cited in Chapter 6.)

[304] De Ze Mo and R. Tijdeman, *Exponential Diophantine equations with four terms*, Indag. Math. (N.S.) 3 (1992), 47–57. (Cited in Chapter 6.)

[305] H. L. Montgomery and P. J. Weinberger, *Notes on small class numbers*, Acta Arith. 24 (1973/74), 529–542. (Cited in Chapter 3.)

[306] M. J. Mossinghoff, G. Rhin, and Q. Wu, *Minimal Mahler measures*, Experiment. Math. 17 (2008), 451–458. (Cited in Chapter 10.)

[307] M. R. Murty and H. Pasten, *Modular forms and effective Diophantine approximation*, J. Number Theory 133 (2013), 3739–3754. (Cited in Chapter 8.)

[308] M. R. Murty and P. Rath, Transcendental Numbers. Springer-Verlag, New York, 2014. (Cited in Chapter 3.)

[309] M. R. Murty and S. Wong, *The abc-conjecture and prime divisors of the Lucas and Lehmer sequences*. In: Number theory for the millennium, III (Urbana, IL, 2000), 43–54, A K Peters, Natick, MA, 2002. (Cited in Chapter 7.)

[310] T. Nagell, *Lϕsning til oppgave nr 2, 1943, s. 29*, Nordisk Mat. Tidskr. 30 (1948), 62–64. (Cited in Chapter 4.)

[311] ———, *The Diophantine equation $x^2 + 7 = 2^n$*, Ark. Math. 4 (1960), 185–187. (Cited in Chapter 4.)

[312] ______, Introduction to number theory. Second edition. Chelsea Publishing Co., New York, 1964. (Cited in Appendix C.)

[313] ______, Collected papers of Trygve Nagell. Vol. 1–4, Edited by Paulo Ribenboim, Queen's Papers in Pure and Applied Mathematics 121, Queen's University, Kingston, ON, 2002. (Cited in Chapter 4.)

[314] M. Nair, *A note on the equation $x^3 - y^2 = k$*, Quart. J. Math. Oxford (2) 29 (1978), 483–487. (Cited in Chapter 13.)

[315] W. Narkiewicz, Elementary and analytic theory of algebraic numbers. Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. (Cited in Appendices B & C.)

[316] Yu. Nesterenko, *Linear forms in logarithms of rational numbers*. In: Diophantine approximation (Cetraro, 2000), 53–106, Lecture Notes in Math., 1819, Springer, Berlin, 2003. (Cited in Chapter 2.)

[317] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. 45 (1949), 502–509. (Cited in Appendix B.)

[318] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*. Séminaire Bourbaki, 30 (1987-1988), Exposé No. 694, 22 p. (Cited in Chapter 8.)

[319] J. Ouaknine and J. Worrell, *Ultimate Positivity is decidable for simple linear recurrence sequences*. In: Automata, languages, and programming. Part II, 330–341, Lecture Notes in Comput. Sci., 8573, Springer, Heidelberg, 2014. (Cited in Chapter 13.)

[320] ______, *Positivity problems for low-order linear recurrence sequences*. In: Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, 366–379, ACM, New York, 2014. (Cited in Chapter 13.)

[321] O. Perron, Die Lehre von den Ketterbrüchen. Teubner, Leipzig, 1929. (Cited in Appendix A.)

[322] A. Pethő, *Über die nichtlineare Diophantische Approximation von quadratischen, algebraischen Zahlen*, J. Number Theory 12 (1980), 334–338. (Cited in Chapters 4 & 13.)

[323] ______, *Perfect powers in second order linear recurrences*, J. Number Theory 15 (1982), 5–13. (Cited in Chapter 6.)

[324] ______, *Perfect powers in second order recurrences*. In: Topics in Classical Number Theory, Proceedings of the Conference in Budapest 1981, Colloq. Math. Soc. János Bolyai 34, pp. 1217–1227, North–Holland, Amsterdam, 1984. (Cited in Chapter 3.)

[325] ______, *Diophantine properties of linear recursive sequences. II*, Acta Math. Acad. Paedagog. Nyházi. (N.S.) 17 (2001), 81–96. (Cited in Chapter 3.)

[326] ______, *Fifteen problems in number theory*, Acta Univ. Sapientiae, Mathematica, 2 (2010), 72–83. (Cited in Chapter 3.)

[327] P. Philippon, *Quelques remarques sur des questions d'approximation diophantienne*, Bull. Austral. Math. Soc. 59 (1999), 323–334. (Cited in Chapter 8.)

[328] ———, *Addendum à quelques remarques sur des questions d'approximation diophantienne*, Bull. Austral. Math. Soc. 61 (2000), 167–169. (Cited in Chapter 8.)

[329] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*. In: New advances in transcendence theory (Durham, 1986), 280–312, Cambridge Univ. Press, Cambridge, 1988. (Cited in Chapter 1.)

[330] ———, *Formes linéaires de logarithmes sur les groupes algébriques commutatifs*, Illinois J. Math. 32 (1988), 281–314. (Cited in Chapter 1.)

[331] S. S. Pillai, *On* $a^x - b^y = c$, J. Indian Math. Soc. (N.S.) 2 (1936) 119–122, 215. (Cited in Chapter 4.)

[332] ———, *On the equation* $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. 37 (1945), 15–20. (Cited in Chapter 4.)

[333] I. Pink, *On the Diophantine equation* $x^2 + (p_1^{z_1} \cdots p_s^{z_s})^2 = 2y^n$, Publ. Math. Debrecen 65 (2004), 205–213. (Cited in Chapter 6.)

[334] A. J. van der Poorten, *Effectively computable bounds for the solutions of certain Diophantine equations*, Acta Arith. 33 (1977), 195–207. (Cited in Chapter 6.)

[335] ———, *Linear forms in logarithms in the* p*-adic case*. In: Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), pp. 29–57. Academic Press, London, 1977. (Cited in Chapters 1 & 8.)

[336] ———, *An introduction to continued fractions*, Diophantine analysis (Kensington, 1985), 99–138, London Math. Soc. Lecture Note Ser. 109, Cambridge Univ. Press, Cambridge, 1986. (Cited in Appendix A.)

[337] A. J. van der Poorten and H. P. Schlickewei, *The growth condition for recurrence sequences*, Macquarie University Math. Rep. 82-0041 (1982). (Cited in Chapters 3 & 13.)

[338] L. P. Postnikova and A. Schinzel, *Primitive divisors of the expression* $a^n - b^n$ *in algebraic number fields*, Mat. Sbornik 75 (1968), 171–177 (in Russian); English translation in Math. USSR Sbornik 4 (1968), 153–159. (Cited in Chapter 7.)

[339] D. Poulakis, *A note on Schmidt's conjecture*, Bull. Austral. Math. Soc. 96 (2017), 191–195. (Cited in Chapter 13.)

[340] K. Ramachandra, *A note on Baker's method*, J. Austral. Math. Soc. 10 (1969), 197–203. (Cited in Chapter 9.)

[341] K. Ramachandra, T. N. Shorey, and R. Tijdeman, *On Grimm's problem relating to factorisation of a block of consecutive integers*, J. Reine Angew. Math. 273 (1975), 109–124. (Cited in Chapters 5 & 13.)

[342] ———, *On Grimm's problem relating to factorisation of a block of consecutive integers. II*, J. Reine Angew. Math. 288 (1976), 192–201. (Cited in Chapters 5 & 13.)

[343] S. Ramanujan, *Question 464*, J. Indian Math. Soc. 5 (1913), 120. (Cited in Chapter 4.)

[344] G. Rémond, *Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink*. Panoramas et synthèses 52 (2017), 243–284. (Cited in Chapter 13.)

[345] G. Rémond and F. Urfels, *Approximation diophantienne de logarithmes elliptiques p-adiques*, J. Number Theory 57 (1996), 133–169. (Cited in Chapter 1.)

[346] D. Ridout, *Rational approximations to algebraic numbers*, Mathematika 4 (1957), 125–131. (Cited in Appendix A.)

[347] A. M. Robert, A Course in p-adic Analysis. Graduate Texts in Mathematics 198, Springer–Verlag, New York, 2000. (Cited in Appendix F.)

[348] O. Robert, C. L. Stewart, and G. Tenenbaum, *A refinement of the abc conjecture*, Bull. Lond. Math. Soc. 46 (2014), 1156–1166. (Cited in Chapter 8.)

[349] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20. (Cited in Appendix A.)

[350] N. Saradha and T. N. Shorey, *The equation $(x^n - 1)/(x - 1) = y^q$ with x square*, Math. Proc. Cambridge Philos. Soc. 125 (1999), 1–19. (Cited in Chapters 5 & 6.)

[351] W. H. Schikhof, Ultrametric calculus. Cambridge Studies in Advanced Mathematics, 4. Cambridge University Press, Cambridge, 1984. (Cited in Appendix F.)

[352] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416. (Cited in Chapter 7.)

[353] ______, *On primitive prime factors of Lehmer numbers. I*, Acta Arith. 8 (1962/1963), 213–223. (Cited in Chapter 7.)

[354] ______, *On two theorems of Gelfond and some of their applications*, Acta Arith. 13 (1967), 177–236. (Cited in Chapters 1 & 6.)

[355] ______, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math., 268/269 (1974), 27–33. (Cited in Chapter 7.)

[356] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. 31 (1976), 199–204. (Cited in Chapter 4.)

[357] W. M. Schmidt, Diophantine Approximations and Diophantine equations, Lecture Notes in Math. 785, Springer, Berlin, 1991. (Cited in Chapters 4 & 10 and Appendix A.)

[358] ______, *Integer points on curves of genus* 1, Compositio Math. 81 (1992), 33–59. (Cited in Chapters 4 & 13.)

[359] Th. Schneider, *Transzendenzuntersuchungen periodischer Funktionen*, J. Reine Angew. Math. 172 (1934), 65–74. (Cited in Chapter 1.)

[360] ______, *Arithmetische Untersuchungen elliptischer Integrale*, Math. Ann. 113 (1937), 1–13. (Cited in Chapter 1.)

[361] ______, *Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise*, Math. Ann. 121 (1949), 131–140. (Cited in Chapter 13.)

[362] R. Schoof, Catalan's Conjecture. Universitext. Springer-Verlag London, Ltd., London (2008). (Cited in Chapter 4.)

[363] H. G. Senge and E. G. Straus, PV-*numbers and sets of multiplicity*, Period. Math. Hungar. 3 (1973), 93–100. (Cited in Chapter 3.)

[364] J.-P. Serre, *Dépendance d'exponentielles p-adiques*. In: Séminaire Delange-Pisot-Poitou. Théorie des nombres, Tome 7 (1965-1966) no. 2 , Exposé no. 15, p. 1–14. (Cited in Appendix F.)

[365] ______, Local fields. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. (Cited in Appendix F.)

[366] T. N. Shorey, *On gaps between numbers with a large prime factor. II*, Acta Arith. 25 (1973/74), 365–373. (Cited in Chapter 5.)

[367] ______, *Linear forms in the logarithms of algebraic numbers with small coefficients I*, J. Indian Math. Soc. (N. S.) 38 (1974), 271–284. (Cited in Chapters 2 & 5.)

[368] ______, *Linear forms in the logarithms of algebraic numbers with small coefficients II*, J. Indian Math. Soc. (N. S.) 38 (1974), 285–292. (Cited in Chapters 2 & 5.)

[369] ______, *On the greatest prime factor of $ax^m + by^n$*, Acta Arith. 36 (1980), 21–25. (Cited in Chapter 4.)

[370] ______, *Divisors of convergents of a continued fraction*, J. Number Theory 17 (1983), 127–133. (Cited in Chapters 3 & 13.)

[371] ______, *Some conjectures in the theory of exponential Diophantine equations*, Publ. Math. Debrecen 56 (2000), 631–641. (Cited in Chapter 13.)

[372] T. N. Shorey and C. L. Stewart, *On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences*, Math. Scand. 52 (1983), 24–36. (Cited in Chapters 3 & 6.)

[373] ______, *Pure powers in recurrence sequences and some related Diophantine equations*, J. Number Theory 27 (1987), 324–352. (Cited in Chapter 6.)

[374] T. N. Shorey and R. Tijdeman, *On the greatest prime factors of polynomials at integer points*, Compositio Math. 33 (1976), 187–195. (Cited in Chapter 3.)

[375] ______, *New applications of Diophantine approximations to Diophantine equations*, Math. Scand. 39 (1976), 5–18. (Cited in Chapters 6 & 13.)

[376] ______, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics 87, Cambridge University Press, Cambridge, 1986. (Cited in Preface, Chapters 3, 4 & 6, and Appendices B & C.)

[377] C. L. Siegel (under the pseudonym X), *The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$*, (Extract from a letter to Prof. L. J. Mordell), J. London Math. Soc. 1 (1926), 66–68. (Cited in Chapter 4.)

[378] S. Siksek, *The modular approach to Diophantine equations*. In: Explicit methods in number theory, 151–179, Panor. Synthèses, 36, Soc. Math. France, Paris, 2012. (Cited in Chapter 13.)

[379] J. Silliman and I. Vogt, *Powers in Lucas sequences via Galois representations*, Proc. Amer. Math. Soc. 143 (2015), 1027–1041. (Cited in Chapter 7.)

[380] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237. (Cited in Chapter 7.)

[381] C. M. Skinner, *On the Diophantine equation* $ap^x + bq^v = c + dp^z q^w$, J. Number Theory 35 (1990), 194–207. (Cited in Chapter 6.)

[382] N. P. Smart, The algorithmic resolution of Diophantine equations. London Mathematical Society Student Texts, 41. Cambridge University Press, Cambridge, 1998. (Cited in Chapters 4 & 6.)

[383] C. Smyth, *The Mahler measure of algebraic numbers: a survey*. In: Number theory and polynomials, 322–349, London Math. Soc. Lecture Note Ser., 352, Cambridge Univ. Press, Cambridge, 2008. (Cited in Chapter 10.)

[384] V. G. Sprindžuk, *Concerning Baker's theorem on linear forms in logarithms*, Dokl. Akad. Nauk BSSR 11 (1967), 767–769 (in Russian). (Cited in Chapter 1.)

[385] ———, *Estimates of linear forms with* p*-adic logarithms of algebraic numbers*, Vesci Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk 1968 (1968), 5–14 (in Russian). (Cited in Chapter 1.)

[386] ———, Classical Diophantine Equations, Lecture Notes in Math. 1559, Springer-Verlag, Berlin, 1993. (Cited in Preface and Chapters 4 & 6.)

[387] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. 14 (1967), 1–27. (Cited in Chapter 3.)

[388] ———, *A transcendence theorem for class-number problems*, Ann. of Math. 94 (1971), 153–173. (Cited in Chapter 3.)

[389] ———, *A transcendence theorem for class-number problems. II*, Ann. of Math. 96 (1972), 174–209. (Cited in Chapter 3.)

[390] ———, *Effective estimates of solutions of some Diophantine equations*, Acta Arith. 24 (1973), 251–259. (Cited in Chapter 13.)

[391] ———, *On complex quadratic fields wth class-number two*, Math. Comp. 29 (1975), 289–302. (Cited in Chapter 3.)

[392] C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. 35 (1977), 425–447. (Cited in Chapter 7.)

[393] ———, *Primitive divisors of Lucas and Lehmer numbers*. In: Transcendence Theory: Advances and Applications (Cambridge, 1976), pp. 79–92. Academic Press, London, 1977. (Cited in Chapter 7.)

[394] ———, *On the representation of an integer in two different bases*, J. Reine Angew. Math. 319 (1980), 63–72. (Cited in Chapter 3.)

[395] ———, *On divisors of terms of linear recurrence sequences*, J. Reine Angew. Math. 333 (1982), 12–31. (Cited in Chapter 3.)

[396] ———, *A note on the product of consecutive integers*. In: Topics in Classical Number Theory, Vols. I, II, Colloq. Math. Soc. János Bolyai, Vol. 34 (North-Holland, Amsterdam, 1984), pp. 1523–1537. (Cited in Chapter 3.)

[397] ———, *On sets of integers whose shifted products are powers*, J. Combin. Theory Ser. A 115 (2008), 662–673. (Cited in Chapters 5 & 9.)

[398] ———, *On heights of multiplicatively dependent algebraic numbers*, Acta Arith. 133 (2008), 97–108. (Cited in Chapter 9.)

[399] ———, *On the greatest square-free factor of terms of a linear recurrence sequence*. In: Diophantine equations, 257–264, Tata Inst. Fund. Res. Stud. Math., 20, Tata Inst. Fund. Res., Mumbai, 2008. (Cited in Chapter 3.)

[400] ———, *On divisors of Lucas and Lehmer numbers*, Acta Math. 211 (2013), 291–314. (Cited in Preface and Chapter 7.)

[401] ———, *On prime factors of terms of linear recurrence sequences*. In: Number theory and related fields, 341–359, Springer Proc. Math. Stat., 43, Springer, New York, 2013. (Cited in Chapter 7.)

[402] C. L. Stewart and R. Tijdeman, *On the Oesterlé-Masser conjecture*, Monatsh. Math. 102 (1986), 251–257. (Cited in Chapter 8.)

[403] ———, *On the greatest prime factor of* $(ab+1)(bc+1)(ca+1)$, Acta Arith. 79 (1997), 93–101. (Cited in Chapter 3.)

[404] C. L. Stewart and K. Yu, *On the abc conjecture*, Math. Ann. 291 (1991), 225–230. (Cited in Chapter 8.)

[405] ———, *On the abc conjecture. II*, Duke Math. J. 108 (2001), 169–181. (Cited in Preface and Chapter 8.)

[406] J. Stiller, *The Diophantine equation* $x^2 + 119 = 15 \cdot 2^n$ *has exactly six solutions*, Rocky Mountain J. Math. 26 (1996), 295–298. (Cited in Chapter 7.)

[407] R. J. Stroeker and R. Tijdeman, *Diophantine equations*. In: Computational methods in number theory, Part II, 321–369, Math. Centre Tracts, 155, Math. Centrum, Amsterdam, 1982. (Cited in Chapter 9.)

[408] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. 67 (1994), 177–196. (Cited in Chapter 1.)

[409] L. Szalay, *The equations* $2^n \pm 2^m \pm 2^l = z^2$, Indag. Math. (N.S.) 13 (2002), 131–142. (Cited in Chapter 6.)

[410] Sz. Tengely, *On the Diophantine equation* $x^2 + a^2 = 2y^p$, Indag. Math. (N.S.) 15 (2004), 291–304. (Cited in Chapter 3.)

[411] E. Thomas, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory 34 (1990), 235–250. (Cited in Chapter 4.)

[412] A. Thue, *Ueber Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305. (Cited in Chapter 4.)

[413] ———, *Berechnung aller Lösungen gewisser Gleichungen von der Form* $ax^r - by^r = f$, Kra. Vidensk. Selsk. Skrifter. I. Math. Kl. 2 (1918), 9 pages. (Cited in Chapter 4.)

[414] R. Tijdeman, *On integers with many small prime factors*, Compositio Math. 26 (1973), 319–330. (Cited in Chapter 3.)

[415] ———, *On the maximal distance between integers composed of small primes*, Compositio Math. 28 (1974), 159–162. (Cited in Chapter 3.)

[416] ———, *On the equation of Catalan*, Acta Arith. 29 (1976), 197–209. (Cited in Chapter 4.)

[417] ———, *Applications of the Gel'fond-Baker method to rational number theory*. In: Topics in number theory (Proc. Colloq., Debrecen, 1974), pp. 399–416. Colloq. Math. Soc. Janos Bolyai, Vol. 13, North-Holland, Amsterdam, 1976. (Cited in Chapter 4.)

[418] ———, *Exponential Diophantine equations 1986–1996*, Proceedings of the Number Theory Conference, Eger 1996, 523–539, Eds. Győry, Pethő, Sós. De Gruyter, 1998. (Cited in Chapter 3.)

[419] R. Tubbs, Hilbert's seventh problem. Solutions and extensions. Institute of Mathematical Sciences Lecture Notes, 2. Hindustan Book Agency, New Delhi, 2016. (Cited in Chapter 1.)

[420] N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, Acta Arith. 75 (1996), 165–190. (Cited in Chapter 1.)

[421] ———, Elliptic Diophantine equations. A concrete approach via the elliptic logarithm. De Gruyter Series in Discrete Mathematics and Applications, 2. Walter de Gruyter GmbH & Co. KG, Berlin, 2013. (Cited in Chapter 1.)

[422] N. Tzanakis and B. M. M. de Weger, *How to explicitly solve a Thue–Mahler equation*, Compositio Math. 84 (1992), 223–288. (Cited in Chapter 6.)

[423] M. Ulas, *Some experiments with Ramanujan–Nagell type Diophantine equations*, Glas. Mat. Ser. III 49 (2014), 287–302. (Cited in Chapter 7.)

[424] N. K. Vereshchagin, *The problem of the appearance of a zero in a linear recursive sequence*, Mat. Zametki 38 (1985), 177–189, 347 (in Russian). (Cited in Chapter 13.)

[425] P. A. Vojta, Integral points on varieties. Ph.D. thesis, Harvard University, 1983. (Cited in Chapter 6.)

[426] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. 64 (1995), 869–888. (Cited in Chapter 7.)

[427] ———, *Primitive divisors of Lucas and Lehmer sequences, II*, J. Théor. Nombres Bordeaux 8 (1996), 251–274. (Cited in Chapter 7.)

[428] ———, *Primitive divisors of Lucas and Lehmer sequences, III*, Math. Proc. Cambridge Philos. Soc. 123 (1998), 407–419. (Cited in Chapter 7.)

[429] M. Waldschmidt, *Sur l'équation de Pillai et la différence entre deux produits de puissances de nombres entiers*, C. R. Math. Rep. Acad. Sci. Canada 12 (1990), 173–178. (Cited in Chapter 4.)

[430] ———, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canadian J. Math. 45 (1993), 176–224. (Cited in Chapter 2.)

[431] ______, *On a problem of Mahler concerning the approximation of exponentials and logarithms*, Publ. Math. Debrecen 56 (2000), 713–738. (Cited in Chapter 13.)

[432] ______, Diophantine Approximation on Linear Algebraic Groups. Transcendence Properties of the Exponential Function in Several Variables, Grundlehren Math. Wiss. 326, Springer, Berlin, 2000. (Cited in Preface, Chapters 1, 2, 4, 10 & 13, and Appendix B.)

[433] ______, *Linear independence measures for logarithms of algebraic numbers*. In: Diophantine approximation (Cetraro, 2000), 250–344, Lecture Notes in Math., 1819, Springer, Berlin, 2003. (Cited in Chapters 2 & 13.)

[434] ______, *Open Diophantine problems*, Mosc. Math. J. 4 (2004), 245–305. (Cited in Chapter 13.)

[435] ______, *Perfect Powers: Pillai's works and their developments*. In: Collected works of S. Sivasankaranarayana Plliai, Eds. R. Balasubramanian and R. Thangadurai, Collected Works Series, no. 1, Ramanujan Mathematical Society, Mysore, 2010. (Cited in Chapters 4 & 13.)

[436] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. Math. (2) 62 (1955), 230–236. (Cited in Chapter 7.)

[437] B. M. M. de Weger, *Equal binomial coefficients: some elementary considerations*, J. Number Theory 63 (1997), 373–386. (Cited in Chapter 13.)

[438] B. M. M. de Weger and C. E. van de Woestijne, *On the diameter of sets of almost powers*, Acta Arith. 90 (1999), 371–385. (Cited in Chapter 13.)

[439] ______, *On the power-free parts of consecutive integers*, Acta Arith. 90 (1999), 387–395. (Cited in Chapter 13.)

[440] G. Wüstholz, *A new approach to Baker's theorem on linear forms in logarithms. III*. In: New advances in transcendence theory (Durham, 1986), 399–410, Cambridge Univ. Press, Cambridge, 1988. (Cited in Chapter 1.)

[441] ______, *One century of logarithmic forms*. In: A panorama of number theory or the view from Baker's garden (Zürich, 1999), 1–10, Cambridge Univ. Press, Cambridge, 2002. (Cited in Chapter 1.)

[442] T. Yamada, *A note on the paper by Bugeaud and Laurent "Minoration effective de la distance p-adique entre puissances de nombres algébriques"*, J. Number Theory 130 (2010), 1889–1897. (Cited in Chapters 2, 7 & 12.)

[443] K. Yu, *Linear forms in p-adic logarithms*, Acta Arith. 53 (1989), 107–186. (Cited in Chapters 1 & 2.)

[444] ______, *Linear forms in p-adic logarithms. II*, Compositio Math. 74 (1990), 15–113. (Cited in Appendix B.)

[445] ______, *Linear forms in p-adic logarithms. III*, Compositio Math. 91 (1994), 241–276. (Cited in Chapter 1.)

[446] ______, *p–adic logarithmic forms and group varieties, I*, J. Reine Angew. Math. 502 (1998), 29–92. (Cited in Chapters 1 & 2.)

[447] ———, *p–adic logarithmic forms and group varieties, II*, Acta Arith. 89 (1999), 337–378. (Cited in Chapter 1.)

[448] ———, *Report on p-adic logarithmic forms*. In: A panorama of number theory or the view from Baker's garden (Zürich, 1999), 11–25, Cambridge Univ. Press, Cambridge, 2002. (Cited in Chapter 1.)

[449] ———, *p–adic logarithmic forms and group varieties, III*, Forum Math. 19 (2007), 187–280. (Cited in Chapter 2.)

[450] ———, *p–adic logarithmic forms and a problem of Erdős*, Acta Math. 211 (2013), 315–382. (Cited in Chapter 7.)

[451] K. Yu and L. Hung, *On binary recurrence sequences*, Indag. Math. (N.S.) 6 (1995), 341–354. (Cited in Chapter 7.)

[452] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284. (Cited in Chapter 7.)

[453] W. Zudilin, *A new lower bound for* $\|(3/2)^k\|$, J. Théor. Nombres Bordeaux 19 (2007), 311–323. (Cited in Chapter 6.)

Index

Yann Bugeaud

Linear Forms in Logarithms and Applications

The aim of this book is to serve as an introductory text to the theory of linear forms in the logarithms of algebraic numbers, with a special emphasis on a large variety of its applications. We wish to help students and researchers to learn what is hidden inside the blackbox ‘Baker’s theory of linear forms in logarithms’ (in complex or in *p*-adic logarithms) and how this theory applies to many Diophantine problems, including the effective resolution of Diophantine equations, the *abc*-conjecture, and upper bounds for the irrationality measure of some real numbers.

Written for a broad audience, this accessible and self-contained book can be used for graduate courses (some 30 exercises are supplied). Specialists will appreciate the inclusion of over 30 open problems and the rich bibliography of over 450 references.

ISBN 978-3-03719-183-5

9 783037 191835

www.ems-ph.org